


VEER-O-METALS Pvt. Ltd.

Delivering Excellence



IT Policy

Document Control

 <p>VEER-O-METALS Pvt. Ltd. Delivering Excellence</p>	IT Policy	
	Document Number	VOM/ISMS/IT/ITP/001
	Version Number	1.2
	Effective Date	05.01.2022

IT Policy

Version	1.2
Author	Mrs. Gayathri
Reviewer	Dr. Harsha
Approver	Praneet Kumar
Creation Date	01.04.2019
Last Updated Date	05.01.2022

Disclaimer:

The details presented in this document are the efforts of Veer-o-Metals, hereafter referred to as Veer-o-Metals. The Details are confidential, privileged and only for the information of the intended recipient and may not be used, published, or redistributed without the prior written consent of Veer-o-Metals.

Version No.	Date	Prepared/Modified by	Reviewed By	Approved	Change Details
1.1	01.04.2019	Mrs. Gayathri	Dr. Harsha	Praneet Kumar	
1.2	05.01.2022	Mrs. Gayathri	Dr. Harsha	Praneet Kumar	Logo, Policy change

Administration of this manual

SQA Department is responsible for administering, tracking and communicating this policy and answering any questions that may arise. The Senior Management will be responsible for any interpretation of this Process.

Note to Holders (For Document Control Purpose):

If you receive an electronic copy of this document and print it out or a hard copy, please write your name on the front cover



Contents

1.Introduction	9
1. Information Security	9
1.1. Physical Security.....	10
1.2. Infrastructure Control	10
1.3. Software Controls.....	10
1.4. Back up policy.....	10
1.5. Clear Desk Policy	11
1.6. Clear Screen Policy	12
2. Information Classification Policy.....	12
2.1. Purpose	12
2.2. Procedure.....	13
2.3. Scope of information assets.....	13
2.4. Classification Guideline	13
2.5. Labelling Guideline.....	15
2.6. Instruction on information asset handling.....	15
3. Asset Management	17
3.1. Technology Control	17
3.2. Software Installation	18
3.3. Software usage.....	18
4. Cryptographic Policy	19
4.1. Application	19
4.2. Method.....	19
5. SDLC Policy	20
5.1. Introduction	20
5.2. Definitions	20
5.3. Purpose	20
5.4. Detailed Policy Statement.....	20
5.5. Objectives.....	20
5.6. Guidelines.....	21
5.7. The SDLC Phases.....	21
5.8. Initiation Phase.....	21
5.9. Feasibility Phase	21
5.10. Requirements Analysis Phase	22
5.11. Design Phase	22
5.12. Development Phase	22
5.13. Implementation Phase.....	23
5.14. Operations and Maintenance	23
5.15. Applicability.....	23
5.16. Company Office.....	23
6. Cloud Security Policy	23
6.1. Purpose	23



6.2. Scope	23
6.3. Context	24
6.4. Policy Statements	24
6.5. Data Classification	24
6.6. Select Security Controls	24
7. Storage Media Disposal Policy	28
7.1. Disposal Method	28
7.2. Procedure to Transfer Storage Media	28
7.3. Violation of Policy	29
8. Mobile Device Security Policy	29
8.1. Introduction	30
8.2. Scope	30
8.3. Policy	30
8.4. Technical Requirements	30
8.5. User Requirements	31
8.6. Actions which may result in a full or partial wipe of the device, or other interaction by IT	32
8.7. Use of applications which have access to corporate data	32
9. Teleworking Policy	32
9.1. Introduction	32
9.2. Teleworking security policy scope and purpose	32
9.3. Authorization for teleworking	33
9.4. Provision of teleworking equipment	33
9.5. Security of information while teleworking	34
10. Acceptable Usage Policy	34
10.1. Purpose	34
10.2. Applicability	35
10.3. Information Handling	35
10.4. Computer Use	35
10.5. Internet	36
10.6. Email	37
10.7. Security	37
10.8. Antivirus	38
10.9. Personal Devices	38
11. Access Management	38
11.1. Introduction	38
11.2. Objective	38
11.3. User Registration and Deregistration	39
11.4. Password Policy	40
12. Physical & Environmental Security Policy	43
12.1. Introduction	44
12.2. Physical security	44
12.3. Environmental security	44
13. Change Management Policy	44
13.1. Purpose	44

13.2. Applicability.....	45
13.3. Policy.....	45
14. Backup and Restoration Policy.....	45
14.1. Purpose.....	45
14.2. Scope.....	45
14.3. Objectives.....	46
14.4. Applicability.....	46
14.5. Responsibility.....	46
14.6. Policy.....	46
14.7. Data Retention Policy.....	47
15. Log Management.....	48
15.1. Purpose.....	48
15.2. Clock Synchronization.....	48
15.3. Log identification for Monitoring.....	48
15.4. Log Enabling.....	49
15.5. Log Backup and Rotation.....	49
15.6. Log Monitoring.....	49
15.7. Exceptional Logs.....	49
15.8. Guidelines.....	49
15.9. Following events should be monitored.....	49
15.10. Responsibilities.....	50
16. Information Transfer Policy.....	50
16.1. Objectives.....	50
16.2. Scope.....	50
16.3. Policy.....	50
16.4. Roles and Responsibilities.....	53
16.5. Expectations.....	54
16.6. Enforcement.....	54
17. Secure Development Policy.....	54
17.1. Overview.....	54
17.2. Policy.....	54
18. Supplier Security Policy.....	55
18.1. Purpose.....	55
18.2. Scope.....	55
18.3. Policy Statement.....	56
18.4. Third Parties – Data Protection and Information Security Obligations.....	56
18.5. Contracts.....	57
18.6. Management of supplier relationships.....	57
18.7. Sub-Contracting.....	57
18.8. Supplier Access to Veer-O-Metals Information.....	57
18.9. Public.....	57
18.10. Monitoring Supplier Access to the Veer-O-Metals Network.....	58
18.11. Security Incident Management.....	58
18.12. Notification of a personal data breach to the Commissioner.....	59



18.13. Breaches of Policy	59
19. Incident Management Policy	59
19.1. Purpose	59
19.2. Applicability	60
19.3. Policy	60
20. Information Asset Classification Policy	61
20.1. Purpose	61
20.2. Applicability	62
20.3. Policy	62
21. Bring Your Own Device Policy	63
21.1. Acceptable Use	63
21.2. Devices and Support	64
21.3. Reimbursement	64
21.4. Security	64
21.5. Risks/Liabilities/Disclaimers	65
22. Veer-O-Metals Work from Home Policy	65
22.1. Compliance Requirements	66
22.2. Information Systems Security	66
22.3. Remote Access Control	66
22.4. Alternative Work Sites	67
22.5. Data Protection	67
22.6. Backup and Media Storage	67
22.7. Remote System Management	68
22.8. Information Disposal	68
22.9. System Ownership and Return	69
22.10. VIOLATIONS	69
23. Capacity Usage Management Policy	69
24. Purchase Policy	72
24.1. Introduction	72
24.2. Purchase of Laptops	72
24.3. Purchase of Servers	73
24.4. Purchase of Computer Peripherals	73
24.5. Purchase of Software	73
25. Cloud Security Policy	73
25.1. Purpose	73
25.2. Scope	74
25.3. Context	74
25.4. Policy Statements	74
25.5. Data Classification	74
25.6. Select Security Controls	74
25.7. Risk Assessment	76
25.8. Compliance and disciplinary action	77
25.9. Exceptions	77
26. System Security Policy & Procedures	77

26.1. Purpose	77
26.2. Applicability	77
26.3. Policy	77
26.4. Desktop Computing Security Policy	78
26.5. Windows 8, 8.1 & 10	79
26.6. Computing equipment Replacement Policy.....	79
26.7. End Point System Security Policy	80
26.8. Responsibilities.....	87
26.9. Enforcement.....	89
26.10. Exceptions	89
26.11. Disclaimer.....	89
26.12. Policy Acceptance	90
29. Removal Media Policy.....	96

1.Introduction

Veer-o-Metals IT Policy provides the policies and procedures for selection and use of IT within the business which must be followed by all employees. It also provides guidelines to administer these policies, with the correct procedure to follow.

The IT department of Veer-o-Metals will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

1. Information Security

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important asset of the organization which must be

managed with care. All information has a value to the organization. However, not all this information has an equal value or requires the same level of protection.

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

1.1. Physical Security

Security at the premises, two levels of security are provided at the location. Manned security and the access control system. All employees are provided with a Biometric finger print access. Visitors are required to sign the visitor register at the time of entry and exit.

1.2. Infrastructure Control

UPS, backup power (Generator), air conditioning, smoke/fire detectors, fire extinguishers, waterproofing, fireproof cabinets for vital records, Door access system, and Fire alarm system are installed as preventive measures.

1.3. Software Controls

Operating system (OS) Security and authentication, access control, anti-virus, firewall, Server Application Monitoring, Backup Software system, Remote Deploy System, OS Patch Management system, Port Monitoring, and intrusion detection system available to reduce the impact of outages.

It will be the responsibility of IT Support Team to ensure that this requirement is always followed. Any employee becoming aware of a breach to this security requirement is obliged to notify IT Support Team immediately.

All security and safety of all portable technology, Laptops, Mobiles, Tablets, and other handheld devices will be the responsibility of the employee who has been issued with the Laptops, Mobiles, Tablets, and handheld devices. Each employee is required to ensure the asset is always kept safely to protect the security of the asset issued to them.

In the event of loss or damage, IT Support Team will assess the scenario and determine the cost recovery.

All Laptops, Mobiles, Tablets, and other handheld devices when kept at the office desk is to be secured by password/keypad lock provided by IT department.

1.4. Back up policy

It is the responsibility of the project manager (in case of project data)/ concerned department manager to raise a ticket to IT department stating data to be backed up, its location, frequency for backup etc. Based on the ticket, IT team will take the back up in cloud. IT team is responsible for weekly backup and verify data of all Veer-o-Metals applications, corporate functions data resides in Cloud Storage.

It is the responsibility of IT Support Team to ensure that data back-ups are conducted daily/weekly/monthly, or on-demand and the backed-up data is kept in Cloud.

All technology that has internet access must have anti-virus software installed. It is the responsibility of IT Support Team to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

1.5. Clear Desk Policy

To improve the security and confidentiality of information, the Veer-O-Metals have adopted a clear desk policy for papers and removable storage media, and clear screen policy for information processing facilities. This is to reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours or when areas are unattended.

The main reasons for a clear desk policy are:

- a. A clear desk can produce a positive image when our customers visit the company.
- b. It reduces the threat of a security incident as confidential information will be locked away when unattended.
- c. Sensitive documents left in the open can be stolen by a malicious entity.

All staff, employees and entities working on behalf of Veer-o-Metals are subject to this policy. The responsibilities include:

- a. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day.
- b. Computer workstations must be locked when workspace is unoccupied.
- c. Computer workstations must be shut completely down at the end of the workday.
- d. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- e. File cabinets containing Critical or confidential information must be kept closed and locked when not in use or when not attended.
- f. Keys used for access to Critical or confidential information must not be left at an unattended desk.
- g. Laptops must be either locked with a locking cable or locked away in a drawer.
- h. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- i. Printouts containing Critical or confidential information should be immediately removed from the printer.

- j. Upon disposal Critical or confidential documents should be shredded
- k. Whiteboards containing Critical or confidential information should be erased.
- l. Lock away portable computing devices such as laptops and tablets.
- m. Printer should be cleared of papers as soon as they are printed

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Facilities will do a walkaround every week with a prior intimation to all employees to ensure clear desk policy is adhered well in all the user desks.

1.6. Clear Screen Policy

- a. Veer-o-Metals computers / computer terminals should not be left logged on when unattended and should be password protected.
- b. Computer screens should be angled away from the view of unauthorized persons.
- c. The System Security Lock should be set to activate when there is no activity for a short pre-determined period.
- d. The Windows Security Lock should be password protected for reactivation.
- e. Users should log off or lock their machines when they leave the room.

2. Information Classification Policy

2.1. Purpose

- a. The implementation of Information Security lies in first identifying and enlisting the critical assets of Veer-o-Metals.
- b. To define the criteria for identifying and classifying information assets in non- digital and digital form, information processing hardware, enterprise-wide software assets, services and applications of Veer-o-Metals.
- c. Along with providing an inventory of information assets and their classification, this policy addresses handling of identified critical assets with ownership and accountability. The Information asset classification will provide much needed inputs to the Information Risk Management framework.
- d. The Policy and Procedure for Information Asset Classification is therefore a formal approach in realizing the said purpose.

2.2. Procedure

- a. All Information Assets will be recorded in asset inventory software
- b. The ownership of the Information assets shall rest with the functional head
- c. Apart from the categories mentioned as in section 3.3, should the stakeholder identify any other type of asset, which shall have an impact on business when compromised; such an asset shall also form a part of the inventory. The same rules of classification as listed below shall apply for all such assets.
- d. Valuation of information assets shall consider the Business Impact Parameters (Financial, Operational, Regulatory/Compliance, Competitive and Legal); should they be compromised in any manner.
- e. Data or information shall be categorized as CRITICAL, CONFIDENTIAL, INTERNAL AND PUBLIC

2.3. Scope of information assets

This policy covers all information assets:

- a) Electronic documents and files
- b) Hardcopy – printed material documents
- c) Verbal – phone conversation/VOIP conversation / voicemail
- d) Multimedia – photos / video / pod cast

From whatever source:

- a. Veer-o-Metals Clients
- b. Vendors

2.4. Classification Guideline

Classification Label	Description	Example
----------------------	-------------	---------

Critical	<p>This is information of the highest sensitivity and if revealed to an unauthorized individual or organization, could cause:</p> <ul style="list-style-type: none"> • Severe harm to Veer-o-Metals' financial stability, stakeholders' confidence, corporate image. • Can suffer huge losses in a very short window of time. I.e., reaction time for a competitor or any other adversary can be very small while the impact of the breach will be proportionately very high. 	Digital	Financials and Business performance details, Design Verification (Project Completion Report) Restricted Maps, IPR Files
		Hard Copy	Off take Agreements
		Service	
		Physical	Core Switches, Cloud Servers
Confidential	<p>This information is of high sensitivity. If this information is compromised, it could cause:</p> <ul style="list-style-type: none"> • Financial loss, impact on customer/public confidence or market share, newsworthiness • Adverse impact on Veer-o-Metals' business competitiveness. 	Digital	Manpower Planning Sheet, Provisional operational KPIs and cost
		Hard Copy	Sanctioned Position/Standard Post, Increment & Bonus Letter
		Service	Email
		Physical	Mail Servers, Departmental Hard Disk Drives, Laptops/Tablets
Internal Use	<ul style="list-style-type: none"> • This is information that shall be kept within Veer-o-Metals and not made available to the public. • As a rule, any information available to oneself in business capacity will be considered as internal use, unless expressly stated otherwise. 	Digital	Production Statement, IT Procedure Documents
		Hard Copy	Consolidated Tax Audit Report
		Service	
		Physical	L3 Switches, Employee Laptops and Phones
Public	<ul style="list-style-type: none"> • This category of information asset will include public notices, company articles, and news in the media, published by the Corporate Communications department. 	Digital	Press Release
		Hard Copy	Published Balance Sheet, Finalized Publications
		Service	Veer-o-Metals Public Website
		Physical	Environmental Parameters – Display Panel

2.5. Labelling Guideline

There is no need to label Public or Internal information.

Veer-o-Metals does not prescribe a mandatory labelling system for sensitive and confidential information. The labelling of information with a ‘Confidential’ marker is at the discretion of the information owner/author based on the proportion of the information’s sensitivity and on how the information is intended to be handled and shared.

It is recommended that all personal data (e.g., HR information) is labelled as Confidential but there may be occasions when information (e.g., legal correspondence) is always handled as confidential but the Confidential label may not be practical and is not always required. Information Asset Owners should consider and agree what labelling is appropriate for their information, ensure that where labelling is not used for confidential information the information is still being handled/processed as confidential and communicate this to their teams.

If information is deemed to be confidential or sensitive and if labelling is required, labels should be applied ‘as follows:

a. Document:

- At the footer of the front/title page: Confidential

Within a document: Confidential should be clearly marked at the footer of every page within the document

Save your document on your team’s shared folders

b. Email:

- ‘Confidential’ should be included in the subject line of the email

All attachments deemed to be sensitive or confidential should be marked as above for documents.

2.6. Instruction on information asset handling

Class	Handling Guidelines but not restricted to:
CRITICAL	This information shall be distributed strictly on need-to-know basis and the distribution list shall be restricted.
	The owner of the Information Asset shall have the right to declare the asset has “CRITICAL”
	Access to this information shall be housed in an access control environment and where physical documents are concerned, shall always be protected under lock and key in a separate storage.

	Access to these shall be monitored using surveillance systems.
	Data in motion shall always be encrypted.
	Where possible DLP solution should be implemented to protect the data.
CONFIDENTIAL	This information shall be password protected when stored or being transmitted.
	The owner of the Information Asset shall have the right to declare the asset has "CONFIDENTIAL"
	Access to this information shall be strictly limited and controlled at all times.
	This information shall not be left unattended when not in use, if found, same shall be brought in to the notice of CISO on case-to-case basis.
	Distribution and Reproduction of this information shall be limited and on need-to-know basis. All distributions of such information should be approved by CISO/BISO in black and white.
	Hard copies of this information shall be protected under lock and key when not in use.
	Information in soft form shall always be backed up.
	Hard copies shall also be scanned and maintained as backup.
	Owner shall be responsible for classification, assessment of the risk associated with this information.
	Compromise of this information shall be considered as an incident and is subject to strict disciplinary actions.
	The container of this information shall be treated as critical as the information kept in it.
	This information can be shared (if required and approved) with the third party, provided that there has been an NDA signed by them.
This information shall be disposed of as per the procedures for disposal of information.	
Internal Use	Access to this information shall be limited to Veer-o-Metals employees only.
	All Information Assets by default shall be classified as "internal use"
	This information is meant for internal consumption only, while it can be shared with the third party under NDA.
	Backup of this information shall be based on the business requirement and as stated by the owner.
	Owner shall be responsible for classification, assessment of the risk associated with this information.
	This information shall be disposed of as per the procedures for disposal of information.

PUBLIC	Ensure the correctness and completeness of the information (originated by Veer-o-Metals) when made available for public consumption.
	Information going public is subject to appropriate approval.
	Only identified stakeholders shall have the right to declare an Information Asset as "PUBLIC"

3. Asset Management

This policy provides guidelines for the administration of information technology assets and resources within the business.

3.1. Technology Control

All hardware, software installed, and the license information must be registered on the asset inventory. It is the responsibility of IT Support Team to ensure that this inventory is maintained. The inventory must record the following information:

- a. Tagging of Hardware and software assets and its ownership
- b. What software is installed on every machine
- c. What license agreements are in place for each software package
- d. Renewal dates if applicable.

IT Support Team is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by IT/Management.

IT Support Team is responsible for maintaining adequate technology spare parts and other requirements including Laptops, Wi-Fi access points.

A technology audit is to be conducted annually by SQA to ensure that all information technology policies are being adhered to. IT asset inventory audit to be conducted by IT department every 6 months.

Employee exit formality should be carried out by IT Team as per the clearance form provided by HR Team. IT team will collect all the assets allocated to the employee by referring asset inventory and should revoke Email, VPN and other credentials provided.

Any unspecified technology administration requirements should be directed to IT/Management.

Vulnerability assessment and penetration testing will be conducted for external and Internal IPs to identify technical vulnerabilities and take necessary action to prevent them.



3.2. Software Installation

All software must be appropriately registered with the supplier where this is a requirement. Veer-o-Metals is to be the registered owner of all software. All software installation is to be carried out by IT Support Team.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

3.3. Software usage

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of IT Support Team/concern team manager.

Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.

Unless express approval from IT Support Team is obtained, software cannot be taken home and loaded on a employees' home computer.

Unauthorized software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

IT Team has to conduct half yearly audit to ensure no unauthorized or pirated software installed in the system.

The unauthorized duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorized copies of software will be referred to HR Team for disciplinary action. The illegal duplication of software or other copyrighted works is condemned within this business and IT Support Team is authorized to undertake disciplinary action where and when such event occurs.

Any issues or difficulty in using IT assets like laptop, electronic gadgets, and software applications to be raised to IT support team through ticketing tool. Support team will validate the ticket and assign priority and the same will be updated in the tool. Below the SLAs will be followed by the IT support team in resolving issues

Ticket Priority	SLA
Very High	Within 2hrs
High	Within 6Hrs

Medium	Within 24 hrs.
Low	Within 48 hrs.

4. Cryptographic Policy

Full disk encryption will be rolled out gradually to all computers across the Veer-o-Metals. The encryption software employed for use at the Veer-o-Metals uses the AES 128 bit (Advanced Encryption Standard) which is a symmetric-key encryption with a 128-bit key.

4.1. Application

Full disk encryption will be rolled out to all computers by IT department as part of laptop upgrades via the build process.

- The build process checks the make and model against a list of machines.
- As part of the process the relevant cryptographic key will be written manually.
- Access to the list of the keys in the cloud through which it is restricted to senior level team members.
- Relevant keys for a machine can be obtained from the cloud through formal application to the Server Team where a senior level member of the team will review the request.

4.2. Method

- On encryption of portable storage device, the user will need to set a password for accessing the device. The password for encrypted portable devices must be in line with the Veer-o-Metals' password policy.
- Using the portable device on any other computer after being encrypted will require a password to access it. It is important that local procedures are put in place to ensure that passwords used to encrypt devices are approved by line managers, so that in the event an individual leaves the Veer-o-Metals, access can be gained to the Veer-o-Metals' data. If local procedures for the creation of encryption passwords have not been followed, employees may be asked to provide details of encryption passwords used on all such portable devices.
- Under no circumstances should network or other IT system passwords be disclosed to anyone including the IT department.
- Computers requiring encryption for the protection of vulnerable and sensitive data will use Windows Bit locker encryption and Linux dm-crypt.

5. SDLC Policy

5.1. Introduction

The Company recognizes a responsibility to have a Software Development Life Cycle Policy (SDLC). This policy defines the guidelines as it pertains to Software Development for the Technology Services staff in the Veer-o-Metals.

5.2. Definitions

Software Development Life Cycle – (SDLC) is a process of creating or altering information systems, and the models and methodologies that people use to develop these systems.

5.3. Purpose

The purpose of a SDLC methodology is to provide IT Project Managers with the tools to help ensure successful implementation of systems that satisfy strategic and business objectives. The documentation provides a mechanism to ensure that executive leadership, functional managers and users sign-off on the requirements and implementation of the system. The process provides Project Managers with the visibility of design, development, and implementation status needed to ensure delivery on time and within budget.

5.4. Detailed Policy Statement

The goals of this SDLC approach are to:

Deliver quality systems which meet or exceed customer expectations when promised and within cost estimates.

To provide a framework for developing quality systems using an identifiable, measurable, and repeatable process.

To establish a project management structure to ensure that each system development project is effectively managed throughout its life cycle.

Identify and assign the roles and responsibilities of all involved parties, including functional and technical managers, throughout the system development life cycle.

Ensure that system development requirements are well defined and subsequently satisfied.

5.5. Objectives

The SDLC methodology will help to achieve these goals by:

- Establishing appropriate levels of management authority to provide timely direction, coordination, control, review, and approval of the system development project.
- Ensuring project management accountability.
- Documenting requirements and maintaining traceability of those requirements throughout the development and implementation process.
-
- Ensuring that projects are developed within the current and planned information technology infrastructure.
- Identifying project risks early

5.6. Guidelines

A software application typically undergoes several development lifecycles, corresponding to its creation and subsequent upgrades. Each such development lifecycle constitutes a project. Such projects continue until the underlying technology ages to the point where it is no longer economical to invest in upgrades and the application is considered for either continued as-is operation or retirement.

5.7. The SDLC Phases

The SDLC includes six phases, during which defined work products and documents are created, reviewed, refined, and approved. Not every project will require that the phases be subsequently executed and may be tailored to accommodate the unique aspects of a projects. These phases are described in more detail in the following paragraphs.

5.8. Initiation Phase

The Initiation Phase begins when management determines that it is necessary to enhance a business process through the application of information technology. The purposes of the Initiation Phase are to:

- Identify and validate an opportunity to improve business accomplishments of the district or a deficiency related to a business need
- Identify significant assumptions and constraints on solutions to that need
- Recommend the exploration of alternative concepts and methods to satisfy the need

5.9. Feasibility Phase

The Feasibility Phase is the initial investigation, or brief study of the problem to determine whether the systems project should be pursued. A feasibility study established the context through which the project addresses the requirements expressed in Business Case and investigates the practicality of a proposed solution. The feasibility study is used to determine

if the project should get the go-ahead. If the project is to proceed, the feasibility study will produce a project plan and budget estimates for the future stages of development.

5.10. Requirements Analysis Phase

This phase formally defines the detailed functional user requirements using high-level requirements identified in the Initiation and Feasibility Phases. The requirements are defined in this phase to a level of detail sufficient for systems design to proceed. They need to be measurable, testable, and relate to the business need or opportunity identified in the Initiation Phase. The purpose of this phase is to:

- Complete business process reengineering of the functions to be supported
- Verify what information drives the business process
- What information is generated
- Who generates it?
- Where does the information go?
- Who processes it?
- Develop detailed data and process models including system inputs and outputs
- Develop the test and evaluation requirements that will be used to determine acceptable system performance

5.11. Design Phase

During this phase, the system is designed to satisfy the functional requirements identified in the previous phase. Since problems in the design phase can be very expensive to solve in later stages of the software development, a variety of elements are considered in the design to mitigate risk. These include:

- Identifying potential risks and defining mitigating design features.
- Performing a security risk assessment.
- Developing a conversion plan to migrate current data to the new system.
- Determining the operating environment.
- Defining major subsystems and their inputs and outputs.
- Allocating processes to resources.

5.12. Development Phase

Effective completion of the previous stages is a key factor in the success of the Development phase. The Development phase consists of:

- Translating the detailed requirements and design into system components.
- Testing individual elements (units) for usability.
- Preparing for integration and testing of the IT system.

Integration, system, security, and user acceptance testing is conducted during this phase as well. The user, with those responsible for quality assurance, validates that the functional requirements are met by the newly developed or modified system.

5.13. Implementation Phase

This phase is initiated after the system has been tested and accepted by the user. In this phase, the system is installed to support the intended business functions. System performance is compared to performance objectives established during the planning phase. Implementation includes user notification, user training, installation of hardware, installation of software onto production computers, and integration of the system into daily work processes. This phase continues until the system is operating in production in accordance with the defined user requirements.

5.14. Operations and Maintenance

The system operation is ongoing. Conduct annual review with Stakeholders. The system is monitored for continued performance in accordance with user requirements and needed system modifications are incorporated. Operations continue if the system responds to the organization's needs. When modifications are identified, the system may reenter the planning phase. Identify need for system retirement, data retention.

5.15. Applicability

This policy applies to all major application projects, both new applications and upgrades of existing applications.

Any individual who fails to adhere to this policy will be documented on their employee evaluation and may be subject to disciplinary action up to and including dismissal or expulsion.

5.16. Company Office

For interpretations, resolution of problems and specific situations contact:

- **Policy Authority**

Veer-o-Metals Services Steering Committee

6. Cloud Security Policy

6.1. Purpose

To ensure that the confidentiality, integrity, and availability of the Veer-o-Metals' information is preserved when stored, processed, or transmitted by a third-party cloud computing provider.

6.2. Scope

This policy applies to all cloud computing engagements. All cloud computing engagements must be compliant with this policy.

6.3. Context

Cloud computing is defined by NIST as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. It is composed of five essential characteristics including on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured services. It can be provided at a low-level as hosted infrastructure (IaaS), at a mid-tier level as a hosted platform (PaaS), or at a high level as a software service (SaaS). Cloud providers can use private, public, or hybrid models.

6.4. Policy Statements

The cloud services risk-management framework used by the Veer-o-Metals has the following activities mandated by this policy:

- Step 1: Perform data classification (Statement of Sensitivity).
- Step 2: Perform Threat Risk Assessment on the solution.
- Step 3: Address threats/risks identified by implementing the proper controls.
- Step 4: Continuously monitor and periodically audit systems and services.

6.5. Data Classification

All Veer-o-Metals information under consideration for use in a cloud computing environment must first be classified by the appropriate Information Owner.

- Security controls will be applied based on the Information Classification.
- Any Veer-o-Metals Data containing Personally Identifiable Information must ensure data at-rest resides in India.

6.6. Select Security Controls

Security controls for the proposed solution must be appropriate for the level of data classification. Detailed requirements are specified in Information Protection Security Controls (IPSC) for Classified Data. At minimum, the security controls provided by Cloud Service Providers (CSP) must implement the following:

Standards

CSP must ensure that they are compliant with a widely adopted cloud security standard that is acceptable to government:

ISO/IEC 27017, demonstrated via certification with accreditation.

NIST SP 800-53, demonstrated via certification with accreditation; or

Level 2 of Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Certification.

Compliance

CSP must ensure it can demonstrate compliance with a cloud security standard by way of an annual SOC 2 Type II audit conducted by an independent third-party auditor. CSP must demonstrate compliance with security obligations if they are not covered anywhere else.

Access Control

CSP must implement an access control policy and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts. CSP must identify and segregate conflicting duties and areas of responsibility (e.g., separation of duties). CSP must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts. CSP must enforce a limit of logon attempts and concurrent sessions as well as multi-factor authentication for privileged access.

Passwords

CSP must enforce password length, complexity, and history for password-based authentication. CSP must support multi-factor authentication to allow the province to use it. CSP must support single sign-on technologies for authentication.

Awareness

CSP must ensure that it conducts security awareness and training for employees.

Logging

CSP must retain logs that are sufficiently detailed to determine who did what when for a period of 90 days online. CSP must provide online GUI access to logs. CSP must provide the technical capability to forward the logs to the province. CSP must correlate, monitor, and alert on logs.

Investigations

CSP must retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed. CSP must provide adequate investigative support to the province. CSP must support e-discovery and legal holds to meet needs of investigations and judicial requests.

Time

CSP must ensure that infrastructure is synchronized with Stratum 1-time servers.

Change Control

CSP must implement change controls in accordance with reasonable industry practices. CSP must test changes to the environment as part of the change management process. CSP must not utilize production data in test environments.

Configuration/Patch Management/Best Practices

CSP must have an information security policy based on industry best practices. CSP must harden systems and servers using appropriate industry standards. CSP must secure databases using appropriate industry standards and logically isolate and encrypt Province information. CSP must ensure workstations used in management and provisioning are patched and secured with antivirus. CSP must implement physical security according to industry best practices. CSP must remedy vulnerabilities and patches according to criticality. CSP must ensure that applications and programming interfaces are developed according to industry standards.

CP/DRP

CSP must have a business continuity plan and a disaster recovery plan that are reviewed and tested annually. CSP must conduct backups using appropriate industry standards. CSP must have incident management and incident response plans that are reviewed and tested annually.

Asset Disposal

CSP must dispose of assets according to industry best practices. CSP must dispose of information according to industry best practices.

Threat/Risk Assessments

CSP must conduct threat and risk assessments on new systems or material changes to existing ones. CSP must support the province in completing Security Threat and Risk Assessments (STRAs).

Security Testing

CSP must conduct vulnerability scans for new systems and material changes to existing ones. CSP must conduct web app vulnerability scans for new systems and material changes to existing ones. CSP must conduct penetration tests at least annually.

Security Screening

CSP must screen individuals prior to authorizing access to information systems. CSP must conduct criminal record checks on employees.

Supply Chain

CSP must ensure suppliers and contractors meet or exceed CSP's own security policies.

Encryption

CSP must implement encryption of data in transit and at rest for Province information and provide the technical capability to manage encryption keys.

Logical Separation

CSP must logically isolate the province's information and segregate Province traffic from other tenants and management traffic. CSP must implement security devices between zones.

Technical Controls

CSP must implement firewalls and intrusion prevention. CSP must implement application layer firewalls. CSP must enable Province to enable/configure security controls in the tenancy such as firewall, intrusion prevention, antivirus, and encryption (IaaS). CSP must secure remote access according to industry best practices. CSP must implement distributed denial of service attack protection.

Breach Notification

CSP must notify the province within 24 hours of a potential or actual breach or incident that may affect the province's information. CSP must notify the province of any changes to security policies, procedures, or agreements.

Risk Assessment

A risk management process must be used to balance the benefits of cloud computing with the security risks associated with handing over control to a vendor.

As compliance with one of the cloud security standards acceptable to government is one of the required security controls, a simplified risk assessment process of a successful review by TRB and a successful ISB review of the supplier's Statement of Applicability and recent external auditor's report is sufficient.

All findings by TRB and the TRA must be successfully addressed before approval to proceed may be granted. Monitor Services

Ongoing security compliance monitoring and auditing of the supplier by the Veer-o-Metals Corp must be included in contracts with cloud computing providers.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of Veer-o-Metals policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Authority, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.

7. Storage Media Disposal Policy

The purpose of this policy is to establish a standard for the proper disposal of electronic media containing sensitive data. The disposal procedures used will depend upon the type and intended disposition of the media.

7.1. Disposal Method

Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in many ways as described below.

a. Disposal of Hard drives

Prior to disposal, operable hard drives must be overwritten in accordance with the procedures above. Equipment designated for surplus or other disposal should have a label affixed stating that the hard drive has been properly sanitized.

7.2. Procedure to Transfer Storage Media

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The procedure as below:

a. Transfer of Hard drives within department

Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All electronic media should be sanitized as per standards, however; since the drive is remaining within the department, the hard drive may instead be formatted by IT department prior to transfer. Special recovery tools must be used by an individual to access the data erased by this method; any attempt by an individual to access unauthorized data would be viewed as a conscious violation

b. Sending a hard drive out for repair or data recovery

Gate pass must be filled by the Information Custodian and hand over to the security. A register for inward – outward movement of the media must be maintained by the Administrative Officer.

The vendor repairing or recovering data on the hard drive must sign an appropriate agreement with Veer-o-Metals, ensuring that the vendor will take proper care of the data. Once data is recovered or the hard drive is repaired, the original hard drive must be returned to Veer-O-Metals so that it can be disposed of as per disposal policy

a. Disposal of damaged or inoperable hard drives

The IT department must first attempt to overwrite the hard drive-in accordance with the procedures above. If the hard drive cannot be overwritten, the hard drive must be disassembled and mechanically damaged so that it is not usable by a computer.

b. Transfer of electronic media other than Hard drives within department

Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as USB drives, floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible.

c. Moving electronic media outside Veer-o-Metals

Gate pass must be filled by the Information Custodian and hand over to the security. A register for inward – outward movement of the media must be maintained by the Administrative Officer.

All electronic media other than computer hard drives must be erased, degaussed, or rendered unusable before leaving Veer-o-Metals

7.3. Violation of Policy

If there is a reasonable basis to believe that the proper procedures as outlined in this policy have not been or are not being followed, a report must be filed with the IT Department. If improperly sanitized electronic media is found, then the media should be reported to IT Department.

Any employee found to have violated this policy may be subject to disciplinary action, including but not limited to, termination of employment.

8. Mobile Device Security Policy

8.1. Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the Company (Veer-o-Metals) that supports their use to achieve business goals.

However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure.

This can subsequently lead to data leakage and system infection. Veer-o-Metals has a requirement to protect its information assets to safeguard its customers, intellectual property and reputation. This policy outlines a set of practices and requirements for the safe use of mobile devices and applications.

8.2. Scope

All mobile devices, whether owned by Veer-o-Metals or owned by employees, inclusive of smartphones and tablet computers, that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops.

Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.

Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy

8.3. Policy

8.4. Technical Requirements

8.4.1.1. Devices must use the following Operating Systems: Android 4.2 or later, iOS 6.x or later.

8.4.1.2. Devices must store all user-saved passwords in an encrypted password store.

8.4.1.3. Devices must be configured with a secure password that complies with Veer-o-Metals' password policy. This password must not be the same as any other credentials used within the organization.

8.4.1.4. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department.

8.5. User Requirements

- 8.5.1.1. Users may only load corporate data that is essential to their role onto their mobile device(s).
- 8.5.1.2. Users must report all lost or stolen devices to Veer-o-Metals IT immediately.
- 8.5.1.3. If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with Veer-o-Metals' incident handling process.
- 8.5.1.4. Devices must not be "jailbroken" or "rooted" * or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- 8.5.1.5. Users must not load pirated software or illegal content onto their devices.
- 8.5.1.6. Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source, contact the IT Department.
- 8.5.1.7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patch should be checked for weekly and applied at least once a month.
- 8.5.1.8. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
- 8.5.1.9. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Veer-o-Metals IT immediately.
- 8.5.1.10. The above requirements will be checked regularly and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipeout.
- 8.5.1.11. The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
- 8.5.1.12. Users must not use corporate workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

8.6. Actions which may result in a full or partial wipe of the device, or other interaction by IT

8.6.1.1. A device is jailbroken/rooted.

8.6.1.2. A device contains an app known to contain a security vulnerability (if not removed within a given timeframe after informing the user).

8.6.1.3. A device is lost or stolen.

8.6.1.4. A user has exceeded the maximum number of failed password attempts.

8.7. Use of applications which have access to corporate data

8.7.1.1. Cloud storage solutions: Veer-o-Metals supports the use of the following cloud storage solutions Google cloud storage.

8.7.1.2. The use of solutions other than the above will lead to a compliance breach and the loss of access to the corporate network for the user.

9. Teleworking Policy

9.1. Introduction

This information security policy document sets out high level principles and expectations that apply to teleworking. It is a sub-document of Information Security Policy.

9.2. Teleworking security policy scope and purpose

This policy relates to any arrangement where staff work at an offsite location, on a regular or long-term basis, and which also involves them in:

- Holding significant quantities of confidential Company information offsite, whether in electronic or paper format.
- Or having a type or level of remote access to information or applications on Company's servers which exceeds that which is ordinarily available to all employees.

The purpose of this policy is to ensure that teleworking is undertaken safely from an information security perspective. It is therefore required that information security risks, related to each specific teleworking scheme, are identified assessed and managed.

These other information security policies are particularly relevant to users of mobile computing devices and those handling confidential information outside secure Company locations. They may also therefore be particularly relevant for teleworkers:

- Information Security Policy
- Mobile Security Policy
- Cryptography Policy

9.3. Authorization for teleworking

9.3.1. Only if the Company wishes, and is able, to provide suitable teleworking facilities, may the employees undertake teleworking and only in cases where:

- It is the Company that requires the employees to undertake teleworking, or it has been approved by the management and the IT department, to adopt a formal flexible working arrangement.

9.3.2. Employees must also be authorized by their Head of Departments to undertake teleworking as distinct from other remote working arrangements. This authorization must be recorded by the department.

9.3.3. The teleworking authorization process should involve an assessment of information security risk considering several factors: criticality of the information assets being accessed; confidentiality of information being handled and suitability of the teleworking technology and location.

9.3.4. Those providing or supporting remote access facilities must do so in cooperation and with approval of IT Services. See also:

- Network Management Policy

9.4. Provision of teleworking equipment

- a. Arrangements must be in place to ensure that any Company teleworking solutions that should be provided are fully supported and maintained.
- b. Those responsible for managing provision of teleworking equipment must ensure, on termination of the arrangement, the secure return or disposal of all equipment and information, in electronic and paper form, held by the teleworker.
- c. Procedures relating to correct usage of any teleworking solution provided must be documented and explained to teleworking staff. The solution must support adequate data backup and teleworkers must understand the backup procedure.
- d. Any software used as part of a Company teleworking solution must be appropriately licensed.
- e. Any teleworking equipment which provides remote access to the Company network, and the authentication method that it uses to access Company resources, must be approved by the IT team.
- f. Those responsible for managing provision of teleworking equipment should be mindful that teleworking systems will use an external Internet service provider. It cannot be assumed that behind the scenes technical security measures will be the same as those implemented to help

protect campus network devices and this must be reflected when providing appropriate equipment and support.

- g. Provision and support of teleworking must reliably implement comprehensive information security measures. For details see “Management of mobile computing devices” section in:
 - Mobile device Policy
- h. Where it is unavoidable that a teleworker must handle confidential information, they must be provided with a computer incorporating full disk encryption and where necessary file encryption tools. See:
 - Cryptography Policy

9.5. Security of information while teleworking

- a. Staff, provided with computing and communications equipment for teleworking specifically to protect the security of confidential information, must not put the information at risk by using other less secure equipment.
- b. Teleworking equipment provided by the Company may only be modified or replaced if that has been authorized.
- c. Teleworking equipment supplied by the Company is only to be used by the employee, particularly since others are not bound by Company agreements and policies.
- d. Teleworking staff must ensure that adequate backup procedures for any information held offsite are implemented. It would normally, however, be preferable to remotely access data that is held onsite and already subject to routine backup.
- e. Only when unavoidable should staff take, send or print hardcopies of confidential documents out of secure Company’s locations. Where absolutely necessary to handle confidential hardcopy documents they should be kept in locked cabinets when not attended (clear desk policy), sent by special delivery post, delivered by hand where possible and disposed of by shredding.

10. Acceptable Usage Policy

10.1. Purpose

Information is our most important asset. Each Veer-o-Metals employee needs to be aware about the requirements of information security and the appropriate steps to ensure that the information is protected. This policy lists the minimum expectations from each employee to meet information security compliance requirements.

10.2. Applicability

All Employees, contract workers and vendors working under all departments of Veer-o-Metals.

10.3. Information Handling

- All Veer-O-Metals information assets as defined in the Information Asset Management Policy must be classified and handled in accordance with the Information Classification and Handling Policy and Procedures.

10.4. Computer Use

All users of Veer-O-Metals Computers must always ensure that:

- Authorization has been provided to use the Veer-o-Metals facilities with a Domain username and password provided by the Transformation Service.
- User and System account logon passwords are kept private and not shared, displayed, or communicated to anyone who does not have a legitimate right to that information.
- Veer-o-Metals Veer-o-Metal's information and data is not permanently saved to PC hard drives – in the event of the Veer-o-Metal's network being unavailable, advice should be sought from the Transformation Service.
- Sensitive and personal data is not knowingly saved on the PCs hard drive under any circumstances.
- Data and Information saved to portable devices via a PC is only copied to a Veer-o-Metals approved portable device which is encrypted in accordance with the Veer-o-Metal's Encryption Policy.
- Mobile computing devices such as digital cameras and digital dictation devices etc., must not be treated as data storage devices – however, the Veer-o-Metals accepts that photographs/audio files for Veer-O-Metals purposes can also be classed as data and recommends that any photographs/audio files taken are removed from the device(s) and stored on the Veer-O-Metals network as soon as possible. Unless for work purposes, if fitted with a geotagging (location identification) feature, this should be switched off.
- Screens/computers are locked by users when away from the computer.
- Veer-o-Metal's computer equipment, such as desktops, (except for laptop and other portable devices authorized for mobile use) are not removed from their location without line management and/or approval from the Transformation Service.
- Unauthorized, non-standard equipment is not connected to a computer in any way.

- Software is not installed on Veer-O-Metals IT computer equipment by unauthorized staff (authorized access may include specific duties requiring staff to have administrative access to carry out certain job functions) – any software installed must be (or going through the process of being) placed on the approved software list.
- Veer-O-Metals equipment must not be used to store any personal data such as wedding photos, CV's, music files etc.
- Computers are not mishandled, willfully damaged or tampered with in any way – this includes taking off the PC/laptop case cover or removing of any screws or fixings.
- Any suspicious or unknown equipment near or around PCs/laptops is reported to the Transformation Service.
- Computers are logged off and shut down when not in use for extended periods (i.e., overnight) and monitors are powered off.
- Personal cloud-based IT facilities are not used to store work related information.

10.5. Internet

- Personal use of the Internet is allowed but not during working hours. You can use the Internet before you start work, during your lunchtime, or after work.
- You must not use the Veer-O-Metals Internet or email systems for trading or personal business purposes.
- The Veer-O-Metals has in place a process to block categories of internet sites and individual sites if it is deemed appropriate.
- If you use the Internet to buy goods or services, the Veer-O-Metals will not accept liability for default of payment or for security of any personal information you provide.
- Goods must not be delivered to a Veer-O-Metals address.
- Downloading of video, music files, games, software files and other computer programs - for non-work-related purposes - is strictly prohibited. These types of files consume large quantities of storage space on the system (and can slow it down considerably) and may violate copyright laws.

Many Internet sites that contain unacceptable content are blocked automatically by the Veer-O-Metals systems. However, it is not possible to block all "unacceptable" sites electronically. You must not therefore deliberately view, copy or circulate any material that:

- Is sexually explicit or obscene.
- Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive.

- Contains material the possession of which would constitute a criminal offence.
- Promotes any form of criminal activity.
- Contains images, cartoons or jokes that will cause offence.

Veer-O-Metals records the details of all Internet traffic. This is to protect the Veer-O-Metals and its employees from security breaches, including hacking and to ensure that 'unacceptable' sites are not being visited.

10.6. Email

Personal use of Veer-O-Metals email is not permitted at any time.

It is inappropriate to use your Veer-O-Metals email address for personal use as it may give the impression that any business is on behalf of the Veer-O-Metals.

You must not use the email system in any way that is insulting or offensive. You must not deliberately view, copy or circulate any material that:

- Is a sexually explicit or obscene.
- Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive.
- Contains material the possession of which would constitute a criminal offence.
- Promotes any form of criminal activity.
- Contains unwelcome propositions.
- Involves gambling, multi-player games or soliciting for personal gain or profit.
- Contains images, cartoons or jokes that will cause offence.
- Appears to be a chain letter.
- Brings the Veer-O-Metals in to disrepute or exposes it to legal action.

The Veer-O-Metals routinely produces monitoring information which summarizes email use and may lead to further investigation being undertaken.

10.7. Security

The Veer-O-Metals computer systems are under continuous threat from hackers, virus/malware infections, data, and equipment theft. The Veer-O-Metals must always remain

vigilant to safeguard information and data and to protect the security and integrity of all Veer-O-Metals systems.

Users of all Veer-O-Metals computers and devices must ensure that:

- Computers/devices are not given to any unauthorized persons for safe keeping.
- Computers/devices are not left discarded or unattended in public places.
- All portable mobile computing devices and other IT equipment should not be left unattended in any vehicle at any time.
- Computers/devices must be adequately protected from physical damage.
- Computers/devices are not hired, lent, or given out without authorization from the Transformation Service.
- All Computers/devices which are no longer required, or which have reached the end of useful life must be returned via the line manager to the Transformation Service to be disposed of through the Veer-O-Metals disposal procedure.

10.8. Antivirus

Any warnings visible on screen from the Veer-O-Metals Antivirus/Antimalware software about identified/detected threats from viruses/malware should be reported to the CISO immediately.

10.9. Personal Devices

Personal devices which are not the property of the Veer-O-Metals, including mobile phones, PDAs, digital pens etc., must not be used to record or capture information relating to the Veer-O-Metals and its services.

11. Access Management

11.1. Introduction

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

11.2. Objective

This policy provides guidelines for the administration of providing and revoking the employee access to the allocated systems and applications. The IT manager shall be responsible for the administration of access controls to all company computer systems.

Users who need access to any application or system should raise a ticket to IT department mentioning which access rights (modify/read only) required and how long the access required along with the

department head approval. IT department will provide the access based on the ticket and department head approval.

Each user must be allocated access rights and permissions to computer systems and data that:

- a. Are commensurate with the tasks they are expected to perform.
- b. Have a unique login that is not shared with or disclosed to any other user.
- c. Have an associated unique password that is requested at each login.

User access rights must be reviewed every month by department heads/Project managers to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

11.3. User Registration and Deregistration

For new employees, request for laptop to be raised to IT department by HR through ticketing tool. IT will immediately acknowledge the ticket and will allocate the laptop within 2 working days along with username and password. Employees are requested to change the password immediately after receiving the laptop.

Employee exit formality should be carried out by IT Team as per the clearance form provided by HR Team. IT team should revoke Email, Jira, Bitbucket, Confluence, VPN and other credentials provided to employee along with the assets allocated

Role	Responsibility
IT Team	<ul style="list-style-type: none"> ○ Only provide users with access to services they require and are specifically authorized to use ○ Restrict and control allocation of system privileges ○ Adjust access rights appropriately and in a timely manner when operational changes require it ○ Audit systems for unwanted/redundant accounts ○ Revoke access and de-register user accounts when user leave ○ Users IDs should not be shared ○ User password must never be disclosed to anyone else ○ Access to servers must be provided through secure channel like VPN ○ Role based access must be given to the users (e.g if user wants to view the files, he must be given only read access) ○ Limit the access to root or admin accounts.

	<ul style="list-style-type: none"> ○ Firewall, IPS and other security devices should be in place to restrict the access for unauthorized users.
Employees	<p><u>Each employee:</u></p> <ul style="list-style-type: none"> ○ Shall be responsible for all computer transactions that are made with his/her User ID and password ○ Shall not disclose password to others. Password must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained ○ Should log out when leaving a workstation for an extended period ○ Should not attempt to access the accounts of other users
Project Manager (PM)	<ul style="list-style-type: none"> ○ PM should notify the IT manager promptly whenever an employee leaves the company or transfer to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination ○ Review user access rights regularly
Human Resource (HR)	<ul style="list-style-type: none"> ○ HR should notify the IT department monthly of associate transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

11.4. Password Policy

a) Authentication

For most of systems used at Veer-O-Metals, authentication using a user ID and secure password (in accordance with the steps included in this document) shall be sufficient. In exceptional cases, for example remote access to sensitive Company systems via the Internet, secure two-factor authentication (e.g., user ID and token) shall be deployed.

b) User Categories

- Individual User IDs (Laptops)

All users (except as provided for below) must have unique individual user IDs. This includes use of e-Mail, applications, and system management.

- System User IDs – Network Infrastructure Equipment and Application IDs

Default User IDs and password of newly supplied systems and network devices must be changed by IT Admin while commissioning.

➤ Guest IDs

Guest IDs shall be disabled unless there is a business requirement for them.

c) Password Management

➤ Password communication

- Passwords shall be communicated by email to concern user Passwords may not be left with another person nor left on the user's desk.

➤ Change passwords after first use

- Where passwords are initially selected or reset by Security Administrators, force or tell users to change them at the next logon (where technically possible). This shall be applicable across applications, infrastructure devices and end user systems.

➤ Password reset procedure

Security Administrators shall reset passwords. In these cases, the caller's identity shall be verified by one of the following methods:

- The user sends a request for password reset to the help desk.
- Verify the user and valid reason for resetting the password, such as date of birth, joining date or mobile number.
- If the IT Help Desk is suspicious about the request, contact the user's Line Manager / Head or an IT contact person of the caller's department.

➤ Access to another person's user ID

IT team or Security Administrators shall not reset a password for a user ID that does not belong to the user making the request. In emergency situations, where there would be a significant adverse impact on the organization, passwords may be reset upon the receipt of written (or e-mail) authorization by the project manager or functions head which explains the reason for the access. Access shall only be granted for a short period to retrieve/copy the required information after which access shall be withdrawn. The owner of the user ID shall subsequently be informed of the circumstances. A record of all such cases shall be maintained vide the exception form.

d) Password Standard

- Enforce password history 5 passwords remembered
- Maximum password age 45 days
- Minimum password age 1days
- Minimum password length 8 characters
- Password must meet complexity requirements Enabled

e) Use of Passwords and Passphrases for Remote Access Users

Access to the Veer-O-Metals Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

f) Secure Logon Procedures

- Disable the user ID after 3 unsuccessful logon attempts so that it cannot be accessed until resumed by administrator. Where there are technical or business reasons why this is not enforced, compensating controls shall be introduced, such as an increasing time delay before further logon attempts are allowed. The same shall be deployed for all server and network device access and application database access.
- Minimize displayed information regarding reasons for logon failures. For example, do not display “incorrect password” because this implies that the user ID is correct.
- Passwords must not be displayed on the screen when being entered or changed.
- In cases of known absence on account of sabbatical, health grounds, transfer, the IDs shall be disabled, and passwords reset on the same day, the request is received from the concerned PM/Function head.

g) Privileged Access Rights

Access within software applications, project repository in confluence, services and code repository in bit bucket must be restricted using the security features built into the individual product. Users who need access to raise a ticket to IT department along with the duration for which access required with the proper approval from department head. IT department is responsible for granting access to the information within the system. The access must Be compliant with the User Access Management section (section 4) and the Password section (section 4.2) above.

- a. Be separated into clearly defined roles.
- b. Give the appropriate level of access required for the role of the user.
- c. Be unable to be overridden (with the admin settings removed or hidden from the user).
- d. Be free from alteration by rights inherited from the operating system that could allow unauthorized higher levels of access.
- e. Be logged and auditable.

h) Network Access control

The use of modems on non- Veer-O-Metals owned Laptops connected to the Veer-O-Metals network can seriously compromise the security of the network. No personal gadgets are allowed to access Veer-O-Metals Veer-O-Metals network unless specifically authorized by top management. The normal operation of the network must not be interfered with. Specific approval must be obtained from IT department before connecting any equipment to the network.

For regular operational purpose, all the laptops are connected to WIFI and will be automatically connected when the system is in the premises. Visitors' internet access will be provided based on the ticket raised by the respected project Lead/Manager.

Rapid SSL certification will be implemented to ensure security of the network services.

For EU projects, separate LAN will be created to ensure the compliance of GDPR. For other projects, network segregation will be done based on customer requirements

i) User authentication for external connection

In case of work from home or connecting outside organization premises, a ticket to be raised to IT department. Remote access to the network must be secured by two factor authentications consisting of a username and one other component, for example RSA token, OTP.

j) Operating system access control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the Password section above must be applied. The login procedure must also be protected by:

- a. Not displaying any previous login information e.g., username.
- b. Limiting the number of unsuccessful attempts and locking the account if exceeded.
- c. The password characters being hidden by symbols.
- d. Displaying a general warning notice that only authorized users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g., administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

12. Physical & Environmental Security Policy

12.1. Introduction

The objective of this policy is to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

12.2. Physical security

Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorization to enter such areas are to be provided with information on the potential security risks and the measures used to control them. These security controls will be in accordance with the Access Control Policy.

Server rooms, data centers, offices, and other locations either housing critical information processing facilities or from where such facilities might be accessed must have good physical security. Equipment that supports critical business activities must be physically protected from security threats and environmental hazards and must be sited, or protected, to reduce the risks of damage, interference, and unauthorized access.

12.3. Environmental security

Whether offices or computer rooms, physical security protection should be based on defined perimeters with security enforced at an appropriate level for each one. As far as practicable, only authorized persons should be admitted to such areas and appropriate entry controls should be implemented to achieve this. All Authority employees are required to wear visible identification and should be encouraged to challenge strangers.

Visitors to secure areas should only be granted access for specific, authorized purposes and should be supervised. As security could be compromised by allowing members of the public temporary access for enquiry or delivery purposes, separate enquiry, delivery or loading areas should be provided outside secure areas. Key Information will be protected in accordance with the Information Classification Policy. Laptop computers and mobile equipment will be protected in accordance with the Mobile Computing and Communications Policy.

13. Change Management Policy

13.1. Purpose

The purpose of the Change Management Plan is to define and agree on how changes are to be coordinated within the project and organization. The plan addresses how the project will ensure that the changes are beneficial, determine how the change will occur, and manage the changes as they occur.

13.2. Applicability

All employees, contract workers and vendors working under IT, HR and Admin department of Veer-O-Metals.

13.3. Policy

The purpose of the Change Management Plan is to coordinate changes across the entire project. The plan will address how the project will ensure that the changes are beneficial, determine how the change will occur, and manage the changes as they occur Password controls shall include managing password complexity, periodicity (Change Interval) and length which shall be enforceable by Active Directory implementation or by formal approved process.

- It is assumed that a request for change may occur in many forms – oral or written, direct or indirect, externally, or internally initiated, and legally mandated or optional.
- Veer-O-Metals shall employ a formal mechanism to capture change requests emerging from the business groups and the technology groups.
- All changes before getting executed shall be formally approved by a concerned stakeholder from business and technology groups.
- The Change Requests shall be dealt with, in terms of their importance and impact on the business.
- No changes to the information systems shall be made without valid and authorized change control approval in place.
- A formal review of all changes done to Veer-O-Metals information systems and infrastructure shall be conducted.

14.Backup and Restoration Policy

14.1. Purpose

The policy seeks to define the requirement of necessary and applicable mechanisms for backup and restoration of Veer-O-Metals information assets so that information shall be protected from misuse, theft and loss and be available when required by authorized users.

14.2. Scope

This policy covers all aspects of backup and recovery for Veer-O-Metals data.

14.3. Objectives

The following principles direct this policy

- Proper back up, storage, and handling of data is necessary for Veer-O-Metals to achieve its objective efficiently.
- Veer-O-Metals will act to preserve information relating to its business.
- Veer-O-Metals employees must protect the availability, confidentiality, and integrity of Veer-O-Metals data.

14.4. Applicability

- Location of Veer-O-Metals in India.
- All Employees of Veer-O-Metals in India.

14.5. Responsibility

- This policy applies to all employees, contractors, consultants, and authorized users of Veer-O-Metals. Policy breaches may lead to disciplinary and /or legal action.

14.6. Policy

- Backup of all business data, related application systems and other business critical/confidential applications, wherein the frequency of backup operations and the procedures for recovery and restoration meets the need of the availability of data for the organization. The accepted level of availability should be maintained in case of a disaster or loss of data due to errors and omissions either advertent or inadvertent.
- Archiving of electronic data shall be in accordance with the business, legal and regulatory requirements. Archiving shall be done to ensure that stakeholders have easy access on a need-to-know basis of data / information.
- Data backup strategy and data recovery procedures shall be implemented to ensure that critical business data is never lost under any circumstances and is always available.
- Carriage/ transfer of any media within the premises of the Veer-O-Metals or taking it outside the premises shall be done in a secure way.

- Regular process of back up / restoration and that of BCP / DR shall be done independent of each other; however, necessary protocols shall be followed in their individual execution.
- A suitable platform shall be deployed which will provide DR like back up of the application servers and databases.
- Disposal of backup tapes shall be done in accordance with the environmental legislation prevailing in the country of operations. It shall be supervised to prevent any theft / unauthorized copying from occurring.

14.7. Data Retention Policy

- Data retention defines the policies of persistent data and records management for meeting legal and business data archival requirements; although sometimes interchangeable, not to be confused with the Data Protection Act 1998.
- The different data retention policies weigh legal and privacy concerns against economics and need-to-know concerns to determine the retention time, archival rules, data formats, and the permissible means of storage, access, and encryption.
- In the field of telecommunications, data retention generally refers to the storage of call detail records (CDRs) of telephony and internet traffic and transaction data (IPDRs) by Veer-O-Metals. In the case of government data retention, the data that is stored is usually of telephone calls made and received, emails sent and received, and websites visited. Location data is also collected.
- The primary objective in Veer-O-Metals data retention is traffic analysis and mass surveillance. By analyzing the retained data, Veer-O-Metals can identify the locations of individuals, an individual's associates and the members of a group such as political opponents.
- A data retention policy is a recognized and proven protocol within an organization for retaining information for operational use while ensuring adherence to the laws and regulations concerning them. The objectives of a data retention policy are to keep important information for future use or reference, to organize information so it can be searched and accessed at a later date and to dispose of information that is no longer needed.
- The data retention policies within an organization are a set of guidelines that describes which data will be archived, how long it will be kept, what happens to the data at the

end of the retention period (archive or destroy) and other factors concerning the retention of the data.

- A part of any effective data retention policy is the permanent deletion of the retained data; achieving secure deletion of data by encrypting the data when stored, and then deleting the encryption key after a specified retention period. Thus, effectively deleting the data object and its copies stored in online and offline locations.

15. Log Management

15.1. Purpose

The purpose of this section is to address the log management framework to capture improper behavior of information systems, to foster accountability, and to improve systems management for better availability of IT Systems.

IT team to ensure:

- a. All the systems should be time synchronized.
- b. Logging should be enabled for all devices, servers, end point systems and applications.
- c. Audit trails should be identified and maintained for business-critical transactions/ applications.
- d. Regular log analysis should be conducted on identified servers, devices and laptops
- e. Logs should be backed up for audit purposes.

15.2. Clock Synchronization

- a. IT team should define one system as a clock reference, and it should take reference clock from internet through reliable source.
- b. IT team should set the time of the 'time server' to Indian Standard Time (IST).
- c. Configure all other information systems as NTP client to take the reference clock.

15.3. Log identification for Monitoring

- a. The IT Admin should identify the logs to be monitored and the 'Log Specification' should include
 - Source of Log
 - Types of Logs (Security, System, Application)
 - Frequency of logging
 - Frequency of monitoring
 - Log retention period

15.4. Log Enabling

- a. IT team should enable the logs as per the details mentioned in the 'Log Specification of relevant asset
- b. Adequate size for the log files should be set.

15.5. Log Backup and Rotation

- a. A location specific log server should be used to store logs of all systems.
- b. IT team should ensure that the logs of the information system are maintained in a log book for critical server for 6 months.

15.6. Log Monitoring

- a. IT team should monitor a log as per the frequency mentioned in the 'Log Specification'
- b. IT team should report the findings of the log monitoring to the IT Head

15.7. Exceptional Logs

There are situations where particular events are required to be tracked for specific reasons (e.g. suspected fraudulent behavior). In such a situation, project manager or function head, who require logging of events should send a request to the system Admin. The same should be reviewed by the System Admin & inform the same to CISO.

15.8. Guidelines

- a. Logs to monitor unauthorized access should be enabled on Infrastructure Servers, Production systems.
- b. The following logs should be considered for monitoring of anomalous behavior
 - Network logs such as Firewall logs.
 - Operating System logs such kernel messages, private authentication, mail, emergency messages and boot logs for UNIX/Sun Solaris.

15.9. Following events should be monitored

- Administrative account activities
 - System events
 - Application events
 - Security related events
 - Remote access to the critical hosts
 - Console alerts or messages
- a. Logs should be enabled for at least the following events in case of Operating Systems and Databases

- Record of successful / unsuccessful system access attempts
- Record successful / unsuccessful account management attempts
- Record attempts to modify logs

15.10. Responsibilities

a. The responsibility for implementing this procedure lies with the following personnel

Role	Responsibilities
CISO	Review log monitoring process at least once in 3 months
IT Team	<ul style="list-style-type: none">● Synchronize server clock with 'time server'.● Enable / disable logs as per procedure.● Monitor logging process.● Ensure that logs are copied on central log server.● Ensure backup of central log server.● Prepare and distribute Log monitoring report every month● Review the Log Monitoring report daily● Review the exceptional logs

16. Information Transfer Policy

16.1. Objectives

This policy states the minimum-security requirements for physical transfer of information into, across, and out of the organization, in any format.

16.2. Scope

This policy applies to all employees of the Veer-O-Metals and any Third party that processes the organization information.

16.3. Policy

- recognizes its responsibility to process its information correctly and in line with all legal, regulatory, and internal policy requirements.
- It is the Sender's responsibility to assess risks in what they are intending to do and ensure that all associated risks are adequately understood and covered, and that the transfer is properly authorized.

- Veer-O-Metals staff shall not assume that because someone asks for information that they are authorized or legally entitled to have it. If in doubt, staff shall check with their supervisor/manager.
- Once the sender is sure that, the transfer is legal and necessary then he/she must decide what kind of information is being dealt with. This will determine what level of security is appropriate.
- The sender must consider the various methods / media of transfer available and whether they are appropriate.
- Before any information is transferred, one must:
 - Obtain and document the approval of the Information Owner for transfer for example in the case of using e-mail for transfer the owner is notified by putting him/her in the Veer-O-Metals
 - Ensure that the transfer is necessary and is legal
 - Remove or blackout anything that is not essential for the recipient's purpose, different communities shall be established for different recipients & different purpose.
- Confidential information that affects the business interests of a third party, or for which the sender does not hold copyright e.g. bank details, salary details, contracts, agreements shall be dealt with great care.
- Unauthorized release of confidential information can leave Veer-O-Metals staff open to legal sanction or litigation.
- Public information shall be transferred in the most cost-effective method available by:
 - Seeking the permission of the Department that produced or owns this information before making any transfer, even if the transfer appears harmless.
- For all transfers of personal information, it is essential that the identity and authorization of the recipient has been appropriately authenticated by the sender.
- It is essential that Veer-O-Metals has in place systems to ensure that bulk transfers of personal information are appropriately controlled, implementing appropriate security measures around these transfers.

- All new bulk transfers must be authorized by the Head of Section / Service. He / she will decide whether to authorize the transfer of this information after careful consideration of the content, format, and method of transfer.
- Veer-O-Metals IT shall maintain a log of all routine and ad-hoc transfers of bulk personal information (based on information flows review). For ex. (Active Directory, Applications).
- Electronic mail should be used in accordance with the Email Policy.
- Staff shall avoid distribution of chain emails and any other.
- Personal e-mail accounts (e.g., Hotmail accounts, Gmail) must not be used for transferring official / confidential information.
- All Veer-O-Metals staff and contractors shall ensure that the name and e-mail address of the recipient are correct.
- Email message must contain disclaimers and clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- The Sender shall check with the recipient that his / her e-mail system will not filter out or quarantine any attachments transferred by email.
- The sender must check at an appropriate time that the email and any attachments sent to the recipient has been transferred successfully, and report any issues to Head of section/manager.
- Ensure that the information within the e-mail is stored in the agreed format for the record type i.e., in line with professional record keeping guidelines.
- Any removable devices used for information transfer should be scanned for viruses and malware.
- On occasions, when information may need to be transferred in person, careful consideration must be given to all the potential security and confidentiality risks involved. Actions taken to mitigate such risks should be agreed upon and documented.
- Staff shall ensure the following if certain circumstances demand the transfer of information via Fax.

- The sender must check that the Fax number is correct and that the receiver is awaiting transmission.
- For any confidential information, the number must be double-checked by a colleague before transmission and telephone contact must be maintained throughout transmission.
- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine and a clear requirement to securely destroy the message when no longer required.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her direct supervisor/manager.
- Confidential information shall not be stored or transferred using SMS or other way on mobile phones.

16.4. Roles and Responsibilities

- Sender (Veer-O-Metals Staff): The Sender is responsible for ensuring the following requirements of this Policy are met.
 - Assessing the confidentiality of information to be sent.
 - Ensuring that the identity and authorization of the recipient has been formally confirmed and documented.
 - Obtaining the consent of the Data Owner for the transfer of information.
 - Ensuring that the information is sent and tracked in an appropriate manner.
- IT Auditor
 - The IT Auditor in the Internal Audit section will monitor and audit departments to ensure compliance with all statutory and regulatory obligations, and internal policies.
- Section Heads and Supervisors
 - Departmental managers are responsible for ensuring that this Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing, or funding are communicated back to their strategic directors in a timely manner.

- Individual employees
 - Individual employees will be responsible for familiarizing themselves with this Policy and ensuring that any information transfer for which they are responsible is done in a compliant manner.
 - Individual employees must report any suspected or actual security breaches related to data transfer in line with the Veer-O-Metals Incident Management Policy.

16.5. Expectations

Exceptions from this policy may be granted by Chief Security Officer, Veer-O-Metals Manager, or Technical Support Supervisor, on a case-by-case basis, after Demonstration of sufficient business need and Completion of a risk assessment by information security team.

16.6. Enforcement

The Information Security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

17. Secure Development Policy

17.1. Overview

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

17.2. Policy

Secure development is a requirement to build up a secure service, architecture, software, and system. Within a secure development policy, the following aspects should be put under consideration:

- security of the development environment.
- guidance on the security in the software development lifecycle.
- Security in the software development methodology.
 - secure coding guidelines for each programming language used.
 - security requirements in the design phase.

- security checkpoints within the project milestones.
 - secure repositories
 - security in the version control.
 - required application security knowledge.
 - Developers' capability of avoiding, finding and fixing vulnerabilities.
- Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use.
 - Developers should be trained in their use and testing, and code review should verify their use. If development is outsourced, the organization should obtain assurance that the external party complies with these rules for secure development.

18. Supplier Security Policy

18.1. Purpose

The purpose of this policy is to put in place procedures so that contracts and dealings between the Veer-O-Metals and third-party suppliers have acceptable levels of data protection and information security in place to protect personal data.

18.2. Scope

The scope of this policy applies to contracts, service arrangements, grant awards and partnership agreements that involve IT solutions or provision of services which require access to, or the processing of, personal data for the delivery and/or support of Veer-O-Metals and business functions.

The term 'processing of personal data' within this policy refers to either: -

- The storing, handling, processing, or retention of data including personal data related to the Veer-O-Metals information e.g., employee, elected member, and client records. Examples include, but not limited to, the procurement of major IT solutions for Payroll etc. or
- The storing, handling, processing or retention of data - including personal data related to/associated with the services commissioned by the Veer-O-Metals. Examples of which include Public Health contracts.

18.3. Policy Statement

Veer-O-Metals has robust and well-established procurement processes which are designed to ensure solutions and services procured are cost effective, maintain the confidentiality, availability and integrity of information, and are fit for purpose. It is fore important that throughout the procurement and subsequent contractual period the Veer-O-Metals and its providers are clear on the Veer-O-Metals expectations in terms of data protection, information security and supplier responsibilities.

18.4. Third Parties – Data Protection and Information Security Obligations

- The security of information is fundamental to the Veer-O-Metals compliance with current data protection legislation and a key focus in its ISO27001 risk assessment, procurement, and management strategy.
- The Veer-O-Metals uses a risk based and proportionate approach to how information assets should be protected. Having procurement processes which align with identified information asset risks helps to ensure that solutions are procured, which are able to provide the level and quality of information security required by the Veer-O-Metals and current data protection legislation. To assess the level of risk, all projects which involve the collection, processing or storage of personal data are required to be supported by the completion of a privacy impact assessment (PIA). PIAs will be applied to new projects or revisions of existing projects. The Veer-O-Metals will identify the need for a PIA at an early stage and build this into project management or other business processes. The client department (Commissioner) will be responsible for creating the PIA and submitting the completed document to the Information Governance Group (IGG) for monitoring purposes. Additional guidance can be found in the Veer-O-Metals PIA Procedures.
- Two procurement approaches have, therefore, been developed for use in the procurement of contracts and the awarding of grants awards/ partnership agreements which include personal data. The use of these approaches is driven by the nature of the service, its integrity to the service that is required, and the sensitivity, volume and risk associated with the information held.
 - Major IT solutions and contracts that involve the processing and / or retention of high volume of personal data.
 - Contract, grant awards and partnership agreements where the use, processing and retention of data is incidental to the service being provided.

18.5. Contracts

- All Veer-O-Metals contracts shall clearly define each party's data protection and information security responsibilities toward the other by detailing the parties to the contract, effective date, functions, or services being provided (e.g., defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the classification of the data, various additional information security controls may be incorporated within the contract in addition to those set out either in Appendix A or B dependent upon the nature of the service provision. The DPB includes details on the Veer-O-Metals
- obligations in terms of contractual requirements with data processors:
- The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following—
 - a. The subject-matter and duration of the processing.
 - b. The nature and purpose of the processing.
 - c. The type of personal data and categories of data subjects involved.
 - d. The obligations and rights of the controller and processor.

18.6. Management of supplier relationships

During the period of the contract or relationship term, the Veer-O-Metals will manage the arrangement with the third-party supplier to ensure data protection and Information Security standards are maintained.

18.7. Sub-Contracting

The Veer-O-Metals will include appropriate contractual obligations to ensure that any sub-contractor engaged by a third-party supplier is required to operate to the same data protection and Information Security standards as the primary contractor.

18.8. Supplier Access to Veer-O-Metals Information

The Veer-O-Metals will allow third party suppliers to access its information and data, where formal contracts and data sharing agreements exist in accordance with current data protection legislation, the Veer-O-Metals' ISMS manual:

18.9. Public

- Accessing the information is an agreed part of the solution/service provided.
- The processing and viewing of information is necessary for maintenance and troubleshooting of the solution being provided.

- Information may need to be reconstructed, repaired or restructured.
- Information has been provided for inclusion in the solution/service by the Veer-O-Metals.
- Information may need to be transferred to other systems or during IT solution upgrades.
- Information may need to be collected with agreement from, and on behalf of, the Veer-O-Metals.

Viewing (i.e., access not agreed by the Veer-O-Metals) of Veer-O-Metals information is not permitted at any time by third party suppliers. Veer-O-Metals information must not be accessed under any circumstances unless formal information sharing agreements or written contractual permissions have been established between the parties which permit this to happen.

The extent of third-party supplier requirements to access Veer-O-Metals information will need to be identified prior to any contractual obligations being established and entered into. The level and type of access to Veer-O-Metals information by third party suppliers must also be formally agreed by the parties. The security requirements for each type of information will be defined within all tender and contract documentation and the security of the information must be handled in accordance with the Veer-O-Metals Information Classification and Handling Policy.

The Veer-O-Metals is very clear that where there is a requirement for the processing of personal data of employees or service users by third parties, information must be treated in accordance with the Veer-O-Metals data protection obligations and requirements to ensure the confidentiality, integrity and availability of all information.

18.10. Monitoring Supplier Access to the Veer-O-Metals Network

IT solutions which are hosted on the Veer-O-Metals network will be subject to periodic checks to ensure that any external access by third party suppliers for support and maintenance is monitored. Once the required work has been undertaken by the third party, access to the account will be disabled and the password changed. Each instance of support and maintenance connections required by the third-party supplier will need to be formally approved by the Veer-O-Metals before being provided.

18.11. Security Incident Management

Third party suppliers will be expected to have appropriate security incident management procedures in place, which correspond to the level of service being provided, sensitivity of the data and GDPR requirements. The extent of these responsibilities will be specified in the contract or data sharing agreement. Third party suppliers will be required to notify the Veer-O-Metals of any significant security incidents as soon as practical.

18.12. Notification of a personal data breach to the Commissioner

The DPB will introduce a duty on the Veer-O-Metals and its third-party suppliers, to report certain types of data breach to the Information Commissioner's Office. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

As a notifiable breach is required to be reported within 72 hours of an organization becoming aware of it, any such instances must be reported through the Veer-O-Metals Incident Reporting procedure immediately. Failure to do so could result in significant monetary fines being levied on the Veer-O-Metals.

18.13. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Veer-O-Metals information assets, or an event which is in breach of the Veer-O-Metals security procedures and policies. All third-party suppliers contracted to provide, support or access solutions, which enable the Veer-O-Metals to carry out its business functions and deliver its services, have a responsibility to adhere to this policy and all supporting requirements as described and referenced within formal documentation and agreed contractual agreements.

All employees, elected members and volunteers have a responsibility to report security incidents and breaches of this policy within 24 hours of becoming aware of the incident through the Veer-O-Metals Incident Reporting Procedure

In the case of third-party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to IT solutions or suspension/ termination of contractual arrangements. If damage or compromise of the Veer-O-Metals IT solutions or loss of information results from the non-compliance, the Veer-O-Metals will consider legal action against the third party. The Veer-O-Metals will take appropriate measures to remedy any breach of this policy and its associated procedures and guidelines through the relevant contractual arrangements in place or otherwise via statutory processes. In the case of an employee, infringements will be investigated under the Veer-O-Metals disciplinary procedure and progressed as appropriate.

19. Incident Management Policy

19.1. Purpose

- a. The policy seeks to establish a mechanism for capturing events and incidents of IT and Non-IT nature.
- b. To capture evidence thereof, perform root cause analysis, prepare, and take corrective and preventive action, generate learnings and examine cost impacts of these incidents and events.

- c. Always ensure that compliance to all the policies and procedures of the organization is adhered to. To adhere to the required statutory and legal compliances as mandated by the law of the land.

19.2. Applicability

All employees, contract workers and vendors working under IT, HR and Admin department of Veer-O-Metals.

19.3. Policy

- a. To understand as to how this policy shall manifest, it is imperative that one understands the meaning of an Event, an Incident and Crisis.
- b. An event is defined as: An identified occurrence in a system, service or network indicating a possible breach of security, procedures and safeguards a previously unknown situation that shall be relevant from the point of view of security.
- c. An incident is defined as: A single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening security.
- d. A crisis shall manifest out of an incident if it threatens the safety of the staff and impacts business continuity. Anything else shall be construed/deemed as incidents/events.

Note: For the sake of brevity, this document shall only address incident management process whereas aspects of crises shall be dealt with in Business Continuity Planning / Management.

- e. Veer-O-Metals has developed, communicated, and implemented formal systems and procedures for detecting and reporting incidents. It has been ensured that the incidents and weaknesses are reported in time to the appropriate authorities and corrective actions are taken immediately to contain the damage and avoid the recurrence of such events in future.
- f. Veer-O-Metals has ensured that all the risks related to incident reporting and possible controls to address those risks are identified and mitigated.
- g. Veer-O-Metals has therefore constituted three teams one each for Physical Security, IT. The heads of all these teams shall have one line reporting to the CISO at Veer-O-Metals
- h. All the incidents have been investigated by the identified personnel in IT Department and Physical Security. Evidence relating to a suspected Information Security and/or Physical Security breach shall be formerly recorded, processed, and preserved as per legal or business requirements.

- i. Incidents shall be managed at an Operational, Tactical and Strategic and Executive Level through designated office bearers.
- j. Necessary Incident Management Maps along with Standard Response procedures shall be developed by the respective teams. So also, aspects of problem management shall also be addressed. Corrective and Preventive action shall be applied as an outcome of the problem management process to minimize the occurrence of the incident.
- k. Incident library shall be maintained, reviewed, and updated on a yearly basis.
- l. Veer-O-Metals shall establish a formal disciplinary process for dealing with employees who commit security breaches.
- m. Employees shall be trained on the incident management process from the purview of individual action.

20. Information Asset Classification Policy

One of the fundamental principles of information security is “need to know”. This principle holds that, the information shall be disclosed only to those people who have a legitimate business need for the same.

Inappropriate handling of information assets could expose the Organization to various risks but not restricted to such as reputational, financial, legal, and regulatory/ compliance and those related to competitive advantage

Hence it is necessary to define a policy and procedure, which will facilitate in the identification of risks to information assets at Veer-O-Metals and classify them in the order of merit of their importance and criticality to the business environment.

20.1. Purpose

- a. The implementation of Information Security lies in first identifying and enlisting the critical assets of Veer-O-Metals This policy (Information Asset Classification Policy and Procedure) helps to establish this precursor to optimizing the security framework.
- b. To define the criteria for identifying and classifying information assets in non- digital and digital form, information processing hardware, enterprise-wide software assets, services, and applications of Veer-O-Metals.
- c. Along with providing an inventory of information assets and their classification, this policy addresses handling of identified critical assets with ownership and accountability. The Information asset classification will provide much needed inputs to the Information Risk Management framework.

- d. The Policy and Procedure for Information Asset Classification is therefore a formal approach in realizing the said purpose.

20.2. Applicability

All employees, contract workers and vendors working under IT, HR and Admin department of Veer-O-Metals.

20.3. Policy

- a. Any asset which has a business value is to be considered as an information asset. This will include but not be restricted to; information in digital and non-digital formats, portable media, network infrastructure devices (servers, routers, switches, modems, tape drives, storage devices, load balancers, ids, ips, firewalls), applications, services, desktops, laptops and mobile computing and communication devices, utilities such as power generation, conditioning and distribution equipment, air-conditioning equipment amongst others.
- b. Valuation of information assets shall consider the Business Impact Parameters (Financial, Operational, Regulatory/Compliance, Competitive and Legal); should they be compromised in any manner.
- c. A score shall be assigned for each of the Business Impact Parameters against Business Impact Criteria such as HIGH, MEDIUM, and LOW comprise of point scale of 5, 2 and 0.5 respectively, to arrive at the Risk Impact Class.
- d. The Risk Impact Class shall be categorized as CRITICAL, SIGNIFICANT, MODERATE AND NEGLIGIBLE. The Risk Impact Class (RIC) will lead to the classification of the Information Asset.
- e. All Information generated or in existence shall be clearly identified and an Information Asset Classification (IAC) template shall be drawn up by respective Department Implementer (DI). The IAC shall only be effective after approval from the authorized signatories.
- f. A labeling schema in pursuant to the classification modality will be adopted.
- g. Retention Limits shall be defined for every category of the identified information asset in consonance with the requisite business, regulatory and legal requirements.
- h. The term 'owner' for an information asset is an individual or department which has a management approval and hence responsibility for controlling the production, development, maintenance, use and security of an asset. The owners shall set the security requirements for information assets and shall be responsible for communicating those requirements to all the custodians.

- i. Custodians shall be those who are the authorized employees/departments who shall have the custody of the Information Asset.
- j. There shall be a formal review mechanism to ensure that the listing of all Information Assets along with their valuation and classification is current, accurate and relevant.
- k. To measure the effectiveness of the process of the maintenance of the inventory of the Information Assets, stakeholders shall be evaluated against the metrics, which have been defined. Corresponding actions and records shall form as supporting elements of the compliance process.
- l. Any exception shall be managed through a formal process.

21. Bring Your Own Device Policy

- Veer-O-Metals grants its employees the privilege of purchasing and using Laptops, smartphones, and tablets of their choosing at work for their convenience. Veer-O-Metals reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.
- This policy is intended to protect the security and integrity of Veer-O-Metals data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.
- Veer-O-Metals employees must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network.

21.1. Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of Veer-O-Metals
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to...
- Devices' camera and/or video capabilities are/are not disabled while on-site.
- Devices may not be used at any time to:
 - Store or transmit illicit materials
 - Store or transmit proprietary information belonging to another company
 - Harass others
 - Engage in outside business activities
 - Etc.

- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
- The following apps are not allowed: (apps not downloaded through iTunes or Google Play, etc.)
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- Veer-O-Metals has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

21.2. Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

21.3. Reimbursement

- The company will/will not reimburse the employee for a percentage of the cost of the device (include the amount of the company's contribution), or the company will contribute X amount of money toward the cost of the device.
- The company will a) pay the employee an allowance, b) cover the cost of the entire phone/data plan, c) pay half of the phone/data plan, etc.
- The company will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

21.4. Security

- To prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's strong password policy is Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- After five failed login attempts, the device will lock. Contact IT to regain access.
- Rooted (Android) or jail broken (iOS) devices are strictly forbidden from accessing the network.

- Employees are automatically prevented from downloading, installing, and using any app that does not appear on the company's list of approved apps.
- Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if
 - the device is lost,
 - the employee terminates his or her employment,
 - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

21.5. Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to always use his or her devices in an ethical manner and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Veer-O-Metals reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

22. Veer-O-Metals Work from Home Policy

Remote Working Privileges – All employees working at home or at alternative sites must be specifically granted this privilege by the employee's manager or a member of the Information Technology Department.

Remote Working Agreement –All Veer-O-Metals employees who are approved to work from remote locations must first sign an agreement to abide by all Veer-O-Metals remote worker policies, procedures, and standards. The agreement should be reviewed and signed annually.

Remote Working Configuration – All critical Veer-O-Metals Employees are granted remote access using Open VPN configured by the IT Department.

22.1. Compliance Requirements

Software License Restrictions – Remote workers must follow software licensing restrictions and agreements on all software used to process Company information at alternative work sites.

Remote Working Information Security Policies – Remote workers must follow Veer-O-Metals information security policies at remote work sites, including the Acceptable Use of Assets Policy.

22.2. Information Systems Security

Approved Remote Worker Equipment – Employees working on Veer-O-Metals business at alternative work sites must use Veer-O-Metals -provided computer and network equipment unless other devices have been approved by the Information Security Department.

Personally-Owned Information systems – Remote workers must not use their own mobile computing devices, computers, computer peripherals, or computer software for Veer-O-Metals Security

Solutions teleworking business without prior authorization from their supervisor.

Setting Date and Time – Remote workers must diligently keep their remote computers' internal clocks synchronized to the actual date and time

Your internal IT Security Policy should set out best practice for remote working, including:

- Device hardware standards
- Password management
- Minimum password standard

Malware Protection Software – All systems that access Veer-O-Metals networks remotely must have an anti-malware (anti-virus) package approved by the Information Security Department continually running.

Advanced Endpoint Protection – All systems that access Veer-O-Metals networks remotely must have an endpoint protection software package installed that protects the system from advances threats.

22.3. Remote Access Control

Access Control System – Remote workers must not use a remote computer for Veer-O-Metals business activities unless this same computer runs an access control system along with the VPN approved by the Information Security Department.

Remote Access to Networks – All remote access to Veer-O-Metals networks must be made through approved Remote Access points that are controlled by the Information Technology Department.

Remote Access Procedure

- Open the OpenVPN software in the system tray
- Click on the Connect button

Session Logout – After a remote worker has completed a remote session with Veer-O-Metals computers, the worker must log off and then disconnect, rather than simply disconnecting. Workers using remote communications facilities must wait until they receive a confirmation of their log off command from the remotely connected Veer-O-Metals machine before they leave the computer they are using.

Screen Positioning – The display screens for all systems used to handle Veer-O-Metals sensitive information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means. **Sharing Access and Systems Prohibited** – Remote workers must not share dynamic password token cards, smart cards, fixed passwords, or any other access devices or parameters with anyone without prior approval from the Information Security Department. This means that a remote computer used for Veer-O-Metals business must be used exclusively by the telecommuter. Family members, friends, and others must not be permitted to use this machine

22.4. Alternative Work Sites

Alternative Work-Site Requirements – Before a remote working (telecommuting) arrangement can begin, the worker’s supervisor or manager must be satisfied that an alternative worksite is appropriate for the Veer-O-Metals work performed by the involved worker.

Remote Working Environmental Controls – Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Lockable, Burglar-Resistant Furniture – All workers who must keep sensitive Veer-O-Metals information and mobile devices at their homes to perform their work, must receive from Veer-O-Metals—or otherwise provide—approved lockable cabinets or desks for the proper storage of this information.

22.5. Data Protection

Encryption and Boot Protection – All computers used for remote working (including portables, laptops, notebooks, and other transportable computers) which contain sensitive (Confidential or Secret)

Veer-O-Metals information must consistently employ both hard disk encryption for all data files and boot protection through a password. These two essential controls must be provided through software or hardware systems approved by the Information Security Department.

22.6. Backup and Media Storage

Backup Procedures – Remote workers are responsible for ensuring that their remote systems are backed up on a periodic basis, either automatically through the network or remotely with USB drives or

similar equipment. If network backup is not available or feasible, Veer-O-Metals will provide telecommuters with local backup equipment.

Backup Media Storage – If backups are made locally, telecommuting workers must store copies of these same backups at a secure location away from the remote working site at least every two weeks. If these backups contain sensitive information, the backups must be encrypted using software approved by the Information Security Department [a link to list of approved information security products can be inserted here].

Sensitive Media Marking and Storage – When sensitive information is written external storage media (external drives, CD-RW, USB drive, etc.), the media must be externally marked with the highest relevant sensitivity classification. Unless encrypted, when not in use, this media must be stored in heavy locked furniture. Smart cards and tamper-resistant security modules are an exception to this rule.

22.7. Remote System Management

Changes to Configurations and Software – On Veer-O-Metals -supplied computer hardware, workers must not change the operating system configuration or install new software. If such changes are required, they must be performed by Help Desk personnel with remote system maintenance software.

Changes to Hardware – Remote working computer equipment supplied by Veer-O-Metals must not be altered or added to in any way without prior knowledge and authorization from the Help Desk.

22.8. Information Disposal

Veer-O-Metals Property at Alternative Work Sites – The security of Veer-O-Metals property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable and prudent precautions must be taken to protect Veer-O-Metals hardware, software, and information from theft, damage, and misuse.

Provision of Secure Containers – Workers who must keep Secret or Confidential Veer-O-Metals information at their homes to do their work must have safes or lockable heavy furniture for the proper storage of this information. If these workers do not have such furniture or safes, Veer-O-Metals will loan these items to the telecommuting workers.

Shredders – Remote workers must have or be provided with a shredder to appropriately dispose of printed versions of sensitive information. Shredders that make strips of paper are not acceptable for the disposal of Veer-O-Metals sensitive material. Acceptable shredders make confetti or other small particles.

Paper Records Disposal – All printed copies of sensitive Veer-O-Metals information must be shredded for disposal. Telecommuting workers on the road must not throw away sensitive information in hotel wastebaskets or other publicly accessible trash containers. Sensitive information must be retained until it can be shredded or destroyed with other approved methods.

22.9. System Ownership and Return

Return of Property – If Veer-O-Metals supplied a telecommuter with software, hardware, furniture, information, or other materials to perform Veer-O-Metals business remotely, all such items must be promptly returned to Veer-O-Metals when a telecommuter separates from Veer-O-Metals, or when so requested by the telecommuter’s manager.

Liability for Veer-O-Metals Property – If Veer-O-Metals supplied a telecommuter with software, hardware, furniture, information, or other materials to perform Veer-O-Metals business remotely, Veer-O-Metals assumes all risks of loss or damage to these items unless such loss or damage occurs due to the telecommuter’s negligence. Veer-O-Metals expressly disclaims any responsibility for loss or damage to persons or property caused by or arising out of the usage of such items.

22.10. VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Veer-O-Metals reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Veer-O-Metals does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, Veer-O-Metals reserves the right not to defend or pay any damages awarded against employees or Third Parties that result from violation of this policy.

23. Capacity Usage Management Policy

Capacity management ensures that the information technology processing and storage capacity is adequate to the evolving requirements of the organization in a timely and cost justifiable manner.

The benefits of an effective and efficient Capacity Management Process include:

- Assurance that IT resources are planned and scheduled to match the current and future needs of the business
- Provision of a Capacity Plan that outlines the IT resources and funding (and cost justification) needed to support the business
- Reduction in Capacity-related Incidents through pre-empting performance issues
- Implementation of corrective actions for capacity-related events
- Methods for the tuning and optimizing of the performance of IT Services and Configuration Items
- A structure for planning upgrades and enhancements and estimating future requirements by trend analysis of current Configuration Item utilization and modelling changes in IT Services
- Assurance that upgrades are planned, budgeted, and implemented before SLAs (in terms of availability or performance) are breached
- Financial benefits through avoidance of 'panic' buying.

The policies for Capacity Management at Veer-O-Metals are as follows:

- The Capacity Management process shall identify Capacity requirements based on business plans, business requirements, SLAs and MOU's and risk assessments, and shall be consulted in the development and negotiation of SLA's and MOU's.
- Capacity Plans will be kept on file for 18 months after their expiry date.
- The Capacity Plans will be reviewed at least annually to ensure requirements reflect agreed-upon changes required by the business.
- The Capacity Management process will be subject to Continuous Process Improvement.
- Capacity Management will endeavor to ensure optimal integration with other IT processes.
- The best available demand forecasts should be provided to Capacity Management as soon as they are identified.
- Monitoring, data gathering, analysis, reporting, and reviews will be undertaken consistently in a defined manner, with the data being stored in the Capacity Management Database (CDB).
- The contents of the CDB will be shared with other IT processes.
- The necessary authority will be delegated to the Capacity Management process to initiate actions which ensure required levels of IT Service Capacity and reliability.

Step	Action
Monitor Individual Hardware & Software Components	<p>Ensure that monitoring is functioning as intended for each of the components on which it is installed and activated.</p> <p>Proceed to 3.2 – Collect Data.</p>
Collect Data	<ul style="list-style-type: none"> • Collect the data for the components on which monitoring is installed and activated. • Organize and collate the gathered data to allow for analysis. • Pass this data to the Service Level Management Process, which will perform audits and reviews on the components from the perspective of their current and future capabilities to deliver the service within the parameters agreed-upon by the SLA's. • After the results of the audits or reviews have been returned from Service Level Management, proceed to 3.3 – Perform Preemptive and Reactive Problem Determination.

<p>Perform Preemptive and Reactive Problem Determination</p>	<ul style="list-style-type: none"> ● Review the results of the monitoring or the Reviews/Audits, as well as the details of any Capacity Event if appropriate. ● Determine the probable cause of any actual or potential capacity problems. ● Identify potential solutions to the problems. ● Record the details of this activity ● Proceed to 3.4 - Determine the Effects of Change.
	<ul style="list-style-type: none"> ●
<p>Plan & Budget HW & SW Upgrades and HW Augmentation</p>	<ul style="list-style-type: none"> ● Create a budget for the upgrades or augmentation. ● Create a high-level plan for the upgrade or augmentation. ● Proceed to 3.6 – Balance Services to Use Existing Resources Efficiently and effectively.
<p>Balance Services to Use Existing Resources Efficiently & Effectively</p>	<p>Identify opportunities to perhaps avoid short-term expenditures by balancing resource usage.</p> <p>Should such opportunities be identified, deploy them?</p> <p>Proceed to 3.7 – Evaluate new HW, SW and Personnel Capability</p>
<p>Evaluate new HW, SW & Personnel Capability</p>	<ul style="list-style-type: none"> ● Evaluate the capabilities of any new hardware components which have been introduced into the environment. ● Evaluate the capabilities of any new software which has been introduced into the environment. ● Evaluate the capabilities of personnel to manage the new hardware or software, especially when if those additions have increased the workload. ● Document the results of the evaluations and distribute them to the appropriate personnel. ● Proceed to 3.8 – Finalize & Agree on the Capacity Plan.
<p>Finalize & Agree on the Capacity Plan</p>	<ul style="list-style-type: none"> ● Collate all the required elements for the new or updated Capacity Plan. ● Create or Update the Capacity Plan.



	<ul style="list-style-type: none">● Obtain agreement for the new or updated plan from the appropriate support teams, as well as from the Service Level Manager.● Record the current Capacity Plan in the CDB.● Proceed to Return.
Return	<ul style="list-style-type: none">● Exit the Manage Resource Capacity Requirements procedure and return to the calling process.

24. Purchase Policy

24.1. Introduction

This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money and where applicable integrates with other technology of the business. The objective of this policy is to ensure that there is minimum diversity of hardware within the business.

The purchase of all desktops servers, portable computers, computer peripherals and mobile devices must adhere to this policy. Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

24.2. Purchase of Laptops

The purchase of portable computer systems includes notebooks, laptops, tablets etc. Portable computer systems purchased must run Windows/Linux/Mac and integrate with existing infrastructure.

The minimum capacity of the portable computer system must be:

- a. 1.5 GHz Processor
- b. GB RAM
- c. USB Ports
- d. microphone port, webcam, speakers.

The portable computer system must include the following software:

- a. Office Software, Adobe reader
- b. Skype, Chrome

Any change from the above requirements must be authorized by Project Manager/Delivery Head. All purchases of all portable computer systems must be supported by warranty and be compatible with the business's server system.

24.3. Purchase of Servers

Server systems can only be purchased by IT/Operations Head. Server systems purchased must be compatible with all other computer hardware in the business. All purchases of server systems must be supported by warranty and be compatible with the business's other server systems. Any change from the above requirements must be authorized by IT/Delivery Head.

24.4. Purchase of Computer Peripherals

Computer system peripherals include printers, projectors, and scanners.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business. The purchase of computer peripherals can only be authorized by Operations Head.

All purchases of computer peripherals must be supported warranty and be compatible with the business's other hardware and software systems.

Any change from the above requirements must be authorized by Operations/IT Head.

24.5. Purchase of Software

All software including open source, freeware etc. must be approved IT Support Team prior to the use or download of such software. The approval should be sought by raising IT ticket to IT department

All purchased software must be purchased by Operations Team. All purchases of software must be supported by warranty and be compatible with the business's server and/or hardware system. Any changes from the above requirements must be authorized by Operations/IT Head.

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

If open source or freeware software is required, approval from IT head or delivery head must be obtained prior to the download or use of such software. An IT ticket along with Approval mail should be forwarded to IT department based on which IT personal will start the installation

All open source or freeware must be compatible with the business's hardware and software systems. Any change from the above requirements must be authorized by Operations/IT Head.

25. Cloud Security Policy

25.1. Purpose

To ensure that the confidentiality, integrity, and availability of the Veer-O-Metals information is preserved when stored, processed or transmitted by a third-party cloud computing provider.

25.2. Scope

This policy applies to all cloud computing engagements. All cloud computing engagements must be compliant with this policy.

25.3. Context

Cloud computing is defined by NIST as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. It is composed of five essential characteristics including on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured services. It can be provided at a low-level as hosted infrastructure (IaaS), at a mid-tier level as a hosted platform (PaaS), or at a high level as a software service (SaaS). Cloud providers can use private, public, or hybrid models.

25.4. Policy Statements

The cloud services risk-management framework used by the Veer-O-Metals has the following activities mandated by this policy:

- Step 1: Perform data classification (Statement of Sensitivity);
- Step 2: Perform Threat Risk Assessment on the solution.
- Step 3: Address threats/risks identified by implementing the proper controls.
- Step 4: Continuously monitor and periodically audit systems and services.

25.5. Data Classification

All Veer-O-Metals information under consideration for use in a cloud computing environment must first be classified by the appropriate Information Owner.

- Security controls will be applied based on the Information Classification.
- Any Veer-O-Metals Data containing Personally Identifiable Information must ensure data at-rest resides in India.

25.6. Select Security Controls

Security controls for the proposed solution must be appropriate for the level of data classification. Detailed requirements are specified in Information Protection Security Controls (IPSC) for Classified Data. At minimum, the security controls provided by Cloud Service Providers (CSP) must implement the following:

1. Standards: CSP must ensure that they are compliant with a widely adopted cloud security standard that is acceptable to government:
 - a. ISO/IEC 27017, demonstrated via certification with accreditation.
 - b. Level 2 of Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Certification.
2. Compliance: CSP must ensure it can demonstrate compliance with a cloud security standard by way of an annual SOC 2 Type II audit conducted by an independent third-party auditor. CSP must demonstrate compliance with security obligations if they are not covered anywhere else.
3. Access Control: CSP must implement an access control policy and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts. CSP must identify and segregate conflicting duties and areas of responsibility (e.g., separation of duties). CSP must maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious, or unused accounts. CSP must enforce a limit of logon attempts and concurrent sessions as well as multi-factor authentication for privileged access.
4. Passwords: CSP must enforce password length, complexity, and history for password-based authentication. CSP must support multi-factor authentication to allow the province to use it. CSP must support single sign-on technologies for authentication.
5. Awareness: CSP must ensure that it conducts security awareness and training for employees.
6. Logging: CSP must retain logs that are sufficiently detailed to determine who did what when for a period of 90 days online. CSP must provide online GUI access to logs. CSP must provide the technical capability to forward the logs to the province. CSP must correlate, monitor, and alert on logs.
7. Investigations: CSP must retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed. CSP must provide adequate investigative support to the province. CSP must support e-discovery and legal holds to meet needs of investigations and judicial requests.
8. Time: CSP must ensure that infrastructure is synchronized with Stratum 1-time servers.
9. Change Control: CSP must implement change controls in accordance with reasonable industry practices. CSP must test changes to the environment as part of the change management process. CSP must not utilize production data in test environments.
10. Configuration/Patch Management/Best Practices: CSP must have an information security policy based on industry best practices. CSP must harden systems and servers using appropriate industry standards. CSP must secure databases using appropriate industry standards and logically isolate and encrypt Province information. CSP must ensure workstations used in management and provisioning are patched and secured with antivirus.

CSP must implement physical security according to industry best practices. CSP must remedy vulnerabilities and patches according to criticality. CSP must ensure that applications and programming interfaces are developed according to industry standards.

11. BCP/DRP: CSP must have a business continuity plan and a disaster recovery plan that are reviewed and tested annually. CSP must conduct backups using appropriate industry standards. CSP must have incident management and incident response plans that are reviewed and tested annually.
12. Asset Disposal: CSP must dispose of assets according to industry best practices. CSP must dispose of information according to industry best practices.
13. Threat/Risk Assessments: CSP must conduct threat and risk assessments on new systems or material changes to existing ones. CSP must support the province in completing Security Threat and Risk Assessments (STRAs).
14. Security Testing: CSP must conduct vulnerability scans for new systems and material changes to existing ones. CSP must conduct web app vulnerability scans for new systems and material changes to existing ones. CSP must conduct penetration tests at least annually.
15. Security Screening: CSP must screen individuals prior to authorizing access to information systems. CSP must conduct criminal record checks on employees.
16. Supply Chain: CSP must ensure suppliers and contractors meet or exceed CSP's own security policies.
17. Encryption: CSP must implement encryption of data in transit and at rest for Province information and provide the technical capability to manage encryption keys.
18. Logical Separation: CSP must logically isolate the province's information and segregate Province traffic from other tenants and management traffic. CSP must implement security devices between zones.
19. Technical Controls: CSP must implement firewalls and intrusion prevention. CSP must implement application layer firewalls. CSP must enable Province to enable/configure security controls in the tenancy such as firewall, intrusion prevention, antivirus, and encryption (IaaS). CSP must secure remote access according to industry best practices. CSP must implement distributed denial of service attack protection.
20. Breach Notification: CSP must notify the province within 24 hours of a potential or actual breach or incident that may affect the province's information. CSP must notify the province of any changes to security policies, procedures, or agreements.

25.7. Risk Assessment

A risk management process must be used to balance the benefits of cloud computing with the security risks associated with handing over control to a vendor.

As compliance with one of the cloud security standards acceptable to government is one of the required security controls, a simplified risk assessment process of a successful review by TRB and a successful ISB review of the supplier's Statement of Applicability and recent external auditor's report is sufficient.

All findings by TRB and the TRA must be successfully addressed before approval to proceed may be granted. Monitor Services

Ongoing security compliance monitoring and auditing of the supplier by the Veer-O-Metals must be included in contracts with cloud computing providers.

25.8. Compliance and disciplinary action

In cases where it is determined that a breach or violation of Veer-O-Metals policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Authority, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

25.9. Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.

26. System Security Policy & Procedures

26.1. Purpose

Veer-O-Metals recognizes that its IT Infrastructure is exposed to security risks because of end user computing systems and related software vulnerabilities. The End Point System Security Policy has been formulated to ensure that any unauthorized access to computing systems shall be prevented and the desired security posture shall be established, maintained, and sustained.

26.2. Applicability

All employees, contract workers and vendors working under IT, HR, and Admin department of Veer-O-Metals.

26.3. Policy

IT Team shall be responsible for ensuring that systems are updated and functional with current operating system patches and antivirus updates. The systems shall be hardened, and appropriate maintenance activity shall be carried out for the system(s) to work optimally.

Use of system utilities which may override system or application control shall be done only under authorization.

Each user shall be provided a unique user ID and password. Password management shall be done to ensure that quality and complexity of passwords is maintained. A formal user registration and de-registration process shall be established. The password complexity shall be as stated in the Password Policy and Procedure.

For critical systems, session time out and connection time out shall be enforced wherever possible. If required login procedures for these systems shall be secure and shall comprise of multifactor authentication techniques.

Systems shall be configured such that users shall be able to lock their terminals either manually or automatically to prevent unauthorized access.

Any changes done to the systems shall be through a formal change management process.

- When any changes are done to the operating systems, then the new system shall be tested before deployment by the assigned personnel from the IT Team.
- Suitable tool shall be deployed for managing integrated roll out of OS Patches and AV Updates and initiate remediation measures to remove inconsistencies in deployment.

26.4. Desktop Computing Security Policy

- Maintain up to date and properly configured anti-virus software. Windows machines which are on campus should generally use Antivirus in Managed Mode. Be sure that real-time protection scans all files.
- Don't open any e-mail attachments unless you know the sender AND know that it was intentionally sent to you.
- Use complex passwords. Never write down your passwords or share them with anyone else. SASC staff will never request your password.
- If you share any files from your machine (not recommended in most cases), be certain that access is protected with a complex password.
- Keep backup copies of any important documents. Contact your IT Support for information about data backup systems.
- Periodically check web site of the OS vendor (e.g., Microsoft or Apple) for critical security updates that may need to be applied.
- Insurance regulations for Property Insurance and Claims require that computing equipment be properly secured if it is to be covered for property loss.

26.5. Windows 8, 8.1 & 10

- These versions of Windows provide much more advanced security than previous versions, but only if the machines are configured with appropriate security settings, administered adequately, and kept up to date with operating system patches. These are the following security settings for such machines.
- File and printer sharing should only be enabled after consulting with local support provider.
- For everyday use, a non-administratively enabled account should be used, to minimize possible destructive impact of viruses/worms/Trojan horses etc. which run in the user's context.
- End users should typically not have administrative access to the machine, when they do, it should be through a secondary account not used day to day.
- Local Administrator account will be renamed and set to have a very lengthy (15-20 characters), complex password.
- Guest account will be disabled and have lengthy, complex password set.
- User/Account logon/logoff events will be logged to the Security log.
- Only NTFS partitions will be used, with appropriately secure access permissions set
- Internet Information Server should not be installed.
- Other unneeded network services should be disabled.

26.6. Computing equipment Replacement Policy

- **Policy statement**

All procurement of Veer-O-Metals computing equipment for individual use and work room deployment will be made in accordance with this policy.

- **Turnover cycle**

- Workroom equipment will be replaced on a 36-month cycle to ensure that equipment is maintained under warranty, has a modern look and feel and has a current and sufficient specification to run all required applications with ease. Re-used equipment will be professionally cleaned, re-imaged, and staff data migrated appropriately without need for special user action/involvement.

- **Laptops**
 - Only staff with a particular requirement to work remotely from their office, or who are able to confirm a realizable benefit to the Veer-O-Metals will be provided with a laptop. Where such equipment is provided for their sole use, it will completely replace their desktop computer.

- **Approved Purchase**
 - Our preference is that the computer equipment is purchased from our preferred suppliers as we have negotiated preferential rates and conducted integration testing.

- **Exception Request**
 - An exception requests required for purchases for other than selected models.

- **Out of Warranty Management**
 - Once out of warranty, equipment will be replaced when significant hardware faults make it uneconomic to repair, and the equipment will be written off.

26.7. End Point System Security Policy

The procedure has been structured to address various aspects of end point computing system security and the corresponding measures / roles which need to be considered for creating a secure access environment. The areas covered in this procedure include

1. Induction of New Systems
2. New Applications, Programs or Updates
3. Hardening of Systems
4. Connection to Local Area Network
5. Connecting to Wireless Network
6. Terminal Timeout
7. Security from malicious code
8. Security of System Documentation and Configuration files
9. Maintenance of Systems
10. Data Protection

11. Patch Management
12. Use of systems utilities and other utility software
13. User DO's and DON'Ts

1. Induction of New Systems

Induction of new systems shall be done as per the procedure defined.

2. New Applications, Programs or Updates

- The users shall not be allowed to download any new application or programs without an approval from the Head of the department, preceded by HoD justification and approval.
- If there is a need of a new application or program, the user shall submit the request to his Department Head and process shall be followed as per Software Copyright Compliance Procedure.
- The Antivirus Administrator shall install the required application or program in the test environment; scan it for viruses and send his approval if the application is free of viruses. Intimate the IT Helpdesk to install the application on user machine.

3. Hardening of Systems

- The Information Security Team shall be responsible for preparing of the Hardening Checklists for desktops, laptops, smart phones, tablets and blackberry phones, Devices. The IT Team shall deploy these checklists.
- The IT Team shall ensure that only required necessary applications and services are installed as per the hardening checklist. The actual hardening of the systems shall be carried out either by the IT Helpdesk personnel or through a dedicated team within the IT Team.
- The IT Team shall identify the patches required to be applied. The deployment of these patches shall be done through the IT Helpdesk.
- Only necessary network protocols, services and ports shall be enabled, which are required by the applications and operating system(s) being used.
- Access to system files on laptops shall be restricted as per Logical Access Control Policy and Procedure. The same shall hold true smart phones, PDAs and Blackberry phones as well.

- Access to system and application files shall be blocked for all users through the hardening activity conducted. Essentially for this aspect to be effective all drives shall be partitioned into a minimum of two partitions e.g., C and D in which C drive shall have OS and other related applications and D drive shall have data.
- Unwanted shares shall be removed. File and directory sharing shall be restricted to authorized personnel by applying appropriate file and directory access permissions.
- The IT Team shall prepare a report confirming, conformation to the Hardening Check list and record exceptions (with reasons). Exceptions if any shall be escalated and necessary approvals sought from the concerned HOD and Information Security Team Head as per business requirement.
- The Information Security Team shall periodically conduct audit of hardening activity and submit its report to the IT Team for them to prepare a Corrective and Preventive Action Plan which shall be executed with 90% compliance. This activity shall be done either through a tool or manually on a quarterly basis or when a new system is inducted into the network.

4. Connection to Local Area Network

- The following procedure shall be followed before laptops, desktops, smart phones, tablets belonging to Veer-O-Metals are connected to LAN:
 - Check to see if the device is registered for use in the Veer-O-Metals network.
 - Check for latest Antivirus definitions
 - Check and ensure that only licensed software is installed on the machines
 - In case of machines with critical data, the hard drive shall be encrypted.
 - IT Team shall assign the IP Addresses for the machines.
 - IT Team shall ensure that the system is hardened as per the baseline security standard at Veer-O-Metals

5. Connecting to Wireless Network

- The requestor shall fill in the Access Request form and submit the form to the Head of the Department (HOD).
- The Head of the Department (HOD) shall forward the form to IT dept. for approval.
- After the approval has been received, the network team shall grant the required access by issuing a joiner ID.
- IT dept. shall assist the user to connect to the wireless network with the joiner ID.
- A certificate for authentication shall be installed on the user system for future authentication requirements.
- The user shall use his domain credentials to connect to the wireless network points in Veer-O-Metals
- The Wi-Fi user group at Veer-O-Metals shall not have administrative user access.

6. Terminal Timeout

- The IT helpdesk shall configure inactive terminals for all systems to be 'timed out' after specific time frame of inactivity to prevent unauthorized access. For all laptops it shall be 60 seconds.
- Approved screen savers with passwords shall be used to protect user systems.
- Users shall lock their terminals and activate screen savers with passwords when the terminal is not in use to protect against information theft or modification of data.
- For critical systems there shall also be limitation on connection time enforced which shall prevent unauthorized usage beyond office hours or before regular office hours. Critical systems shall be identified by the Programmed Managers/HODs and connection time and session time out shall be enforced wherever possible.

7. Security from malicious code

- System is protected from Spy-wares, Mal-wares, Mobile codes, destructive Cookies, Active-X controls by using the following controls:
 - Software installation is controlled to laptops which are enforced using active directory.

- Personal firewall is enabled in each laptop and desktops
- Uncontrolled Internet access is not allowed; the content filter mechanism catches hold of Spyware, Malware etc.
- Antivirus software is having Spyware and Malware control inbuilt.

8. Security of System Documentation and Configuration files

- System documentation shall include system configuration files, installation and decommissioning records, records of modifications, modifications done to applications and systems, application documentation.
- As per the valuation cited above for the various categories of systems, the protection shall be in keeping with the classification done as per the Information Asset Classification Policy.
- All system documentation shall be managed by the IT Team.
- Any changes to the system documentation shall be captured through the Change Management Process.
- Any exceptions or deviations shall be through Exceptions and Deviations form as mentioned in the framework.
- Access rights to the machine where system documentation is stored shall be provided to authorize personnel from IT Team.
- Only designated System Administrators shall have edit privileges if necessary other users shall only have read privileges.
- Scheduled backup of system documentation data and configuration files shall be done and tested as well, with a log of the activity being maintained.
- Access to system documentation shall be through formal approval obtained from Head IT only.
- All system documentation shall be stored on a dedicated system with two factor access control. Backup of this system shall be taken once every week.

- System State Backups of critical systems shall be taken once every week and stored on the dedicated machine.
- The repository of system documentation shall be an integral part of the Digital Rights Management.
- Review of changes done to system documentation and system configuration shall be conducted by the person/team having expertise in various device(s) appointed by the Information Security Head with a periodicity of 90 (Ninety) days.

9. Maintenance of Systems

- The IT dept. shall ensure that the backup of the data is taken before any system maintenance activity for laptops. (Refer to Backup, Restoration).
- In case of critical assets, maintenance activities shall preferably be performed in the presence of the asset owner or his/her authorized representative.
- Emergency repair disks shall be maintained for system restoration. The mirror image of the approved standard system configuration shall be used for faster and error free installations.
- The System Administrator shall design the file system keeping the following points in mind
 - Operating system program files, live application program files, device files or hidden directories with program files in them shall not be present in a user's home directory. These shall be installed in a separate file system or partition users have no access to it.
 - Live or production data shall be kept in a separate file system with proper access control.
 - Test / Demo applications shall be installed and tested on a separate server. Live data shall not be given for testing and test data shall be sanitized.
 - A disk quota shall be assigned to the file system for each user, where the user's home directories are kept.
 - Any malfunction of the system shall be logged as an incident.

- Emergency change - Any change deviating from security hardening due to be done in an emergency (having an impact on the security hardening document) which cannot follow the change request procedure shall be approved by department head by mail and or through the Change Request Form.

10. Data Protection

- Use of USB ports, CDs/DVDs shall be restricted permitted in case of business need and after approval from HOD and/or Information Security Team through the exception form.

11. Patch Management

- The IT dept. shall ensure that current OS patches are identified, tested before they are deployed.
- The relevant patches shall be installed on the systems remotely wherever required. Verification of this activity shall be done through a quarterly audit conducted by the Information Security Team and findings submitted to the IT dept. for necessary implementation.
- Patch updates on user machines shall be done either when the system is logged onto or when user decides to shut down or during the non-load hours of the day.
- A tool-based approach shall be deployed to ensure that patch management inconsistencies are ascertained and remediated without manual intervention.

12. Use of systems utilities and other utility software

- The access to systems utilities shall be restricted as per the Logical Access Control Policy and Procedure. In particular, users shall not be given access to the systems utilities.
- Right for installation of software on the systems shall be restricted to System Administrators/IT helpdesk. The same shall be tested by system admin to check if any existing system applications or services or performance is getting affected.

13. User DO's and DON'Ts

- The viruses and malicious code can propagate through different means including emails, USB drives, pen drives, CDS/DVDs, unauthorized software, downloaded

content. The end users have a key role to play in guarding their machines / data against a virus infection

- Users shall follow these guidelines to the utmost extent possible.
- Shall not attempt to change the scanner setting of their computers.
- Shall ensure that virus definitions of the Antivirus scanner are regularly updated on their machines.
- Shall ensure that personal firewall is enabled on their desktop / laptop if connecting to other external or public networks.
- Shall always run the anti-virus software scans before connecting the portable devices to the network.
- Shall not use floppies or CDs from unreliable sources.
- Shall not install and use illegitimate software.
- Shall not accept free software or use software given free with computer magazines, unless this has been approved.
- Shall not browse or download content from unreliable sites on the Internet. These are typically underground and illegal sites.
- Shall always scan the attachments for viruses before downloading them

26.8. Responsibilities

The responsibility for implementing this procedure lies with the following personnel

- **IT- Security Team**

- Harden Systems (desktops, laptops, smart phones, tablets and blackberry phones.).
- Keep track of software patches and apply appropriate patches on systems.
- Enable appropriate access control settings.
- Ensure that system maintenance activity is carried out under their supervision.

- Categorize calls in terms of severe impact, moderate impact and medium impact and report on a monthly basis.
- Call resolutions as per TAT (Turn Around Time) defined in the Incident Management Policy and Procedure.
- Ensure the hardware and software meets the specifications before system induction.
- Label system components and update asset inventory.
- Create users as per Logical Access policy.
- Install software for protection against malicious code.
- Ensure that system administration activities are logged
- **IT-Helpdesk**
 - Log Virus incidents.
 - Report incidents to Antivirus Administrator.
 - Guide users for corrective measures.
 - Install Antivirus software on all systems.
 - Update Antivirus signatures and updates.
 - Install approved applications only.
- **Users**
 - Ensure that their systems have latest patches and are updated through an assurance note from the IT dept.
 - Ensure that their systems have antivirus installed and its signature updated through the icon on the desktop.
 - Ensure that their systems have been hardened by permitting this activity to be completed on their systems by the Infra Team member.

- Ensure that system maintenance activity is carried out under their supervision, if their systems have Critical and Confidential data.
- Lock their terminals when the terminal is not in use.
- Log incidents through the IT Helpdesk.
- Users are expected to report any suspicious activity on their machines to IT-Helpdesk and adhere to this procedure.
- Not download any new application or programs without an approval.
- Follow the dos and don'ts mentioned in this procedure.
- Remove unapproved applications.

26.9. Enforcement

These policies and procedures are applicable for all the employees and contractors of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt in accordance with the disciplinary action process as laid down in the Code of Conduct.

Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this document at any time as per its discretion.

26.10. Exceptions

Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.

Exceptions to the Personnel Security Policy and Procedures shall be allowed at the time of implementation of this policy and procedures or at the time of making any updating to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.

All exception requests shall be submitted by respective HoDs/ BISOs. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.

The CISO shall review all exceptions, as the case may be, every year for validity and continuity.

26.11. Disclaimer

Veer-O-Metals reserves all rights and is the exclusive owner of all intellectual property rights over this Systems Security Policy and Procedures document. This document shall not, either in part or in

full, be reproduced, published, copied, displayed, distributed, transferred, stored in any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent of the Committee. The Systems Security policy and procedure document are meant to be published on the intranet of Veer-O-Metals and/or any other forum as decided by the management of Veer-O-Metals. Anything not specifically stated in this Systems Security policy and procedure document shall not be considered as implied in any manner.

26.12. Policy Acceptance

I hereby acknowledge that I have read and will comply with all the policies

Name of the Employee: _____ Date: _____

Personal No: _____ Location Name: _____

Department: _____ Ph / Extn. No: _____

Email ID: _____

27. Removal Media Policy

29.1 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

29.2 Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Veer-O-Metals and to reduce the risk of acquiring malware infections on computers operated by Veer-O-Metals. Any questions or comments about this policy should be directed to Information Systems.

29.3 Scope

This policy covers all removable media that contains Veer-O-Metals data or that is connected to a Veer-O-Metals network.

29.4 Policy

Veer-O-Metals staff may use removable media in their work computers. Sensitive information should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information. When sensitive information is stored on removable media, it must be encrypted in accordance with the Veer-O-Metals [Acceptable Encryption Policy](#). Exceptions to this policy may be requested on a case-by-case basis by petition to Information Systems.

29.5 Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. Students may be referred to Student Affairs for discipline. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with Veer-O-Metals.

29.6 Definitions

Removable Media

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks not provided by Veer-O-Metals.

29.7 Encryption

Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

29.8 Malware

Malware is defined as software of malicious intent/impact such as viruses, worms, and spyware.

Veer-O-Metals Network

Being connected to a network includes the following:

- If you have a network capable device (ex. laptop) plugged into a Veer-O-Metals owned building, then you are connected to the LAN (local area network).
- If you have a wireless capable device (ex. laptop, iPhone) and connect to Wireless or Secure, then you are connected to the WLAN (wireless local area network).
- If you connect from a computer through the Veer-O-Metals VPN (virtual private network), you are then connected to the LAN (local area network).

29.9 Sensitive Information



Sensitive information is defined as information which, if made available to unauthorized persons, may adversely affect Veer-O-Metals, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers and financial information. The determination of sensitivity is the responsibility of individual departments.