V-Guard Industries Ltd (VGIL)

Information Security Policy

Ver 1.0

Rule Profile		
General	Short title	ISMS- Information Security Policy
	Rule No.	
	Last Revision	1.0
	Approved By	Management Committee
	Reviewed By	Information Security Team
	Prepared By	Deloitte Team
	Period of Validity	Valid From: 01/04/2022
	Summary	This document outlines the information security policy to preserve Confidentiality, Integrity and Availability of systems and information used by V-Guard Industries Limited (VGIL).
	Number of Pages	33 Pages
Respon sibility	Ownership	Information Security Team, CISO
	Distribution List	All V Guard Employees.
	Documentation	This procedure is documented in V Guard Intranet portal
Other Documents	Annexes	
	Changes and Revision history	
	Further Applicable Regulations	

TABLE OF CONTENTS

1 Introduction

This document outlines the information security policy to preserve Confidentiality, Integrity and Availability of systems and information used by V-Guard Industries Limited (VGIL).

2 Objective

The objective of this policy is to provide governance and ensure: -

- The confidentiality, integrity and availability of critical information.
- Critical information is protected from intentional or unintentional - unauthorized access, use, disclosure, modification and disposal.
- All applicable legal, regulatory and contractual requirements with regard to information security are complied.
- All stakeholders adhere to the policy and the Management has rights to take necessary action in case of violation.

3 Scope

This policy applies to all VGIL units, Stakeholders with whom VGIL has entered a business relationship. This policy applies to all information systems (Including IT assets and Shop Floor assets in factories). Stakeholders include employees, vendors, external contractors, External Auditors, Consultants, Authorized Service Providers and other third parties.

VGIL information assets includes data that is owned, sent, received or processed by VGIL and associated hardware, software, media and facilities.

All stakeholders who use, manage, operate, maintain or develop VGIL applications or data must comply with this policy. The policy also applies to all third parties acting on behalf of VGIL and to representatives who are granted authorized access to VGIL and its information assets.

This policy is supported by secondary policies, standards and guidelines, Checklists, Standard Operating Procedures on various domains (As per ISO 27001, ISO 22301 Standards) of documentation comprises the Information Security Management System (ISMS).

4 Responsibilities

The information security team along with business departments shall be responsible for implementation of the information security policy.

CISO along with Information Security Team to ensure all information security policies are documented, reviewed and implemented across VGIL.

In the occurrence of any security incident, the incident report shall be reviewed by the CISO and shall also ensure mitigation activities are in place. Any deviation reports should be reviewed periodically and mitigation activities to be planned.

CISO should also ensure that security awareness is promoted amongst employees on do's and don'ts on information security.

5 Terms and Definitions

Confidentiality: Confidentiality refers to protecting information from being accessed by unauthorized parties.

Integrity: Refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification.

Availability: Refers to ensuring that authorized parties are able to access the information when needed

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Threat: The potential for a source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Severity: Estimated effect if a business asset is lost, disrupted or harmed in some manner.

Occurrence: Probability that a threat will exploit vulnerability and will result in an undesired event for the business.

Asset: An asset is anything that has value to the organization. There are many types of assets including but not limited to, information, software, physical (hardware), services, people and intangibles such as reputation and brand image.

Information System: Application, service, information technology asset, or any other information handling component.

Access Management: Access management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users.

Risk Assessment: identifying and analyzing potential events that may negatively impact individuals, assets, and/or the environment; and making judgments "on the tolerability of the risk on the basis of a risk analysis" while considering influencing factors.

Encryption: The process of translating a message in a way that the resulting message cannot be understood without unscrambling it first. In information processing systems usually accomplished by using a cipher and cryptographic key.

Key: A piece of information that is used as an input for a cryptographic algorithm, such as encryption algorithm, digital signatures or message authentication.

Antivirus: Antivirus is software that protects against computer viruses, a type of malware that self-replicates by inserting its code into other software programs.

Asset Management: Asset management is a systematic process of developing, operating, maintaining, upgrading, and disposing of assets in the most cost-effective manner.

Security incident management: The process of identifying, managing, recording and analyzing security threats or incidents in real-time.

Business continuity management system: Business continuity management system is a management system that bundles interrelated methods, procedures and rules to ensure that critical business processes keep running in the event of damage or emergencies and continuously develops and improves them.

6 Policy compliance

Violation to the Information security policy or standards of acceptable use of VGIL assets and facilities, unauthorized modification or use of information assets violating the business goals or values are considered as a serious offence. Such actions performed by stakeholders may result in disciplinary action including termination of their service and/or action in accordance with local laws. It is the responsibility of Human Resources (HR) to drive the disciplinary action.

Offences of this nature by third party vendors may result in the revocation of their access rights to VGIL' s information, termination of their service contracts, and/or action in accordance with local laws. It is the responsibility of the respective Head of department along with Compliance to drive the disciplinary action.

7 Organization of Information security

7.1 Information Security responsibility

- All stakeholders of VGIL are responsible for the security and protection of information resources over which he or she has control. Resources to be protected include all Physical Assets and Information Assets. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.
- VGIL management will ensure that proper resources are available to work on the information security management system of VGIL. The Information Security Team of VGIL will have the overall responsibility for establishing, implementing, and monitoring VGIL' s Information Security Program and continuously improve the security posture of VGIL.

7.2 Segregation of Duties at VGIL

All business divisions must adopt the principle of segregation of duties to the maximum extent possible. The initiation of an event / task / activity must be separated from its authorization. The following principles must be followed:

- Persons involved in operational functions must not be given additional responsibilities in administration processes and vice versa
- The responsibility for performing a review of the system or process is completely independent from the roles and responsibilities for developing, maintaining, and using the system or process.
- Where segregation of duties is not possible or practical, the process must include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision.

7.3 Contact with Authorities and Special Interest Groups

- The authorized department and/or individuals in the respective locations shall maintain contact with the relevant authorities in case of emergencies such as Fire accident, and other Disaster scenarios.
- Information Security team shall maintain contact and coordinate with the relevant specialist information security forums and professional associations (e.g. Information Systems Audit and Control Association) in order to exchange knowledge as it pertains to the cyber threat landscape.

7.4 Teleworking and Mobile Device Security

- Teleworking shall be enabled based on approval as per VGIL Mobile, Remote working procedure.
- Access to corporate information from personal devices / BYOD of stakeholders should be governed by a software such as an MDM solution that also ensures privacy of non-corporate information. VGIL shall protect & manage only the corporate data and applications that resides on employee's mobile. Corporate data means any data /information asset which is associated to VGIL and which has been created as part of VGIL Business process.
- To prevent unauthorized access, the mobile devices must be password protected using the features of the device and a strong password must be enforced to access the company network.
- Lost or stolen devices must be reported to VGIL's IT team within 24 hours with FIR or as soon as possible, without delays.
- Users should install business related applications from trusted sources in the device.

8 Human Resources Security

8.1 Prior to employment

The Human Resources (HR) department shall ensure that security responsibilities are briefed to every new individual when he/she joins the organization as well as during exit procedures.

HR department shall carry out background verification and reference checks of prospective employees and contractual staff as per the relevant HR policy.

- Screening check prior to employment or immediately after joining.
- Verification of the original identity documentation (Ex: Passport number, Aadhaar number, PAN Card), confirmation of the candidate's current address and confirmation of the candidate's right to work in the country of hire.
- A completeness and accuracy check of the candidate's past three professional experience verification and references checks.
- Basic level criminal record check.
- Verification of claimed academic qualification(s).

The terms and conditions of employment state that the Employees, Contractors and third-party contractors shall need to comply with all rules, regulations, the information security policy and all the procedures laid down by VGIL. The disciplinary actions taken by VGIL if the employee shall disregard these terms and conditions shall also be clearly defined. These terms and conditions shall appear as an annexure or in any other form to the offer letter that shall be signed and accepted by the employee at the time of joining VGIL. The signed and accepted offer letter shall be maintained by the Human Resource Department securely.

Employee on-boarding information shall be communicated by the HR team to respective departments in VGIL.

HR should ensure all employee related information, payroll details, appraisal & performance details etc., are securely handled. All physical documents should be safely stored in fireproof cabinet with physical access control. All digital copies of employee related information should be stored securely, and access should be restricted on a need to know basis. The HR team should follow the organization's defined retention and disposal standards for employee related information.

8.2 During employment

Information Security Awareness Training

The HR department shall ensure that formal Information Security Training is imparted to the employees, contractors and third party contractors at the time of their induction and every year thereafter; and the training program should include relevant sections of VGIL' s Information Security Policy with appropriate Do's and Don'ts that the employees need to practice in their day-to-day work.

Disciplinary process

Formal disciplinary process shall be established to deal with the violation of organizational security policies and procedures. All employees, contractors and third-party contractors shall be required to become familiar and acknowledge compliance with the policies and procedures laid down by VGIL. Disciplinary action shall correspond to the severity of the incident, as determined by an investigation team. Disciplinary actions shall include, but shall not be limited to, loss of access privileges to data processing resources, termination or suspension of employment, civil and/or criminal prosecution, or other actions as deemed appropriate by management.

The Investigation team shall have representatives from:

1) Legal team
2) Human Resources Department
3) Concerned Business Department
4) Information Security Department
5) Based on the severity and nature of the incident, additional stakeholders shall be called for.

Violations of VGIL's information security policy include but shall not be limited to any acts that:

- Expose VGIL to actual or potential monetary loss through the compromise of information security or damage and loss of Information Systems / Resources;
- Involve the disclosure of trade secrets, intellectual property, confidential information, or the unauthorized use of VGIL's data; and
- Involve the use of information for illicit purposes, which shall include violation of any law or regulation.

8.3 Termination or change of employment

HR department should notify to all concerned departments, as soon as the resignation/ separation of an employee is accepted with the last date of employment. IT team may put in place additional monitoring of employee activities during the notice period.

All employees, contractors and third-party contractors are required to return all information assets that are issued to them.

Information security policy and non-disclosure agreements applicability post the termination shall be communicated and signoff shall be obtained from the employee, contractor and third-party contractors during off-boarding process.

Employee, contractor and third-party contractors shall undergo the exit interview and shall need to submit "NO DUE" certificate from all support departments.

9 Asset Management

- All assets shall be clearly identified, documented & regularly updated in the asset register / inventory.
- All assets shall have designated asset owners & custodians.
- All employees shall use company assets as per the acceptable use of assets.
- All assets shall be classified as per the information classification of the organization.
- All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
- All information stored on the organization' s system belongs to the organization, and the organization may inspect all such information at any time, as necessary.

9.1 Acceptable Use of Assets

This outlines the acceptable use of Asset / Information Assets / Systems / Resources of VGIL which includes (but not limited to) all computer equipment, software, hardware, operating systems, storage media, network, electronic mail, internet & intranet, remote access services, telephony systems, mobile computing environment, physical copies / non-digital information and usage / storing / transmission / processing services provided by VGIL.

It also provides expectation around use and protection of corporate and all relevant client information. The "user" of these resources is any person (full-time, part-time and temporary employees, trainees, contractor, consultants and third party) who has access to Information Systems in order to perform for VGIL business related activities. It also includes all personnel affiliated with third parties that use VGIL information.

General Usage of VGIL' s Information Assets

- VGIL Information Assets shall be used for processing data and information relating to VGIL business in course of normal business operations.
- Users shall not attempt to access any data or programs contained on VGIL Information Systems for which they do not have authorization.
- Users are responsible for protecting any corporate information in their possession including that stored on their respective VGIL's workstations, laptops, mobile, servers, personal computing devices, Mobile

Devices and on any physical forms. Users shall not use Information Systems (including internet and email) for any activity with an intent of:
- Discriminating, harassing, vilifying or victimizing others based on gender, race, religious beliefs, disability, political conviction, sexual preferences, age or otherwise.
- Degrading systems performance.
- Depriving an authorized user access to VGIL's information system.
- Attempting to gain additional system access or privileges than allocated.
- Circumventing/Disabling VGIL's information security control measures or non-compliance to VGIL Information Security Policy.
- Installing software programs including freeware and shareware not explicitly authorized by the Head of department and Manager – SYSTEMS.
- Causing physical damage to facility or property.
- Sending unsolicited messages and creating or forwarding of 'chain emails.

- Users shall not take **'Information'** or **'Information Systems'** out of VGIL' s premises without appropriate authorization and valid business justification / purpose.
- Users shall familiarize and follow the VGIL Information Security Policy (and any updates to these). Any doubts or queries shall be raised with their Head of departments or the Information Security team.
- Users shall comply with security directives, guidelines, and polices at all times. Users shall not circumvent or attempt to circumvent any logical or physical security control or guidelines issued by VGIL. Additionally, users shall proactively participate in all security and safety exercises / drills / trainings that may be conducted.
- 'Users' are responsible for the content they store or transmit using VGIL **'Information Systems'** and mobile computing devices. **"Users'** shall respect all copyrights, trademarks and may not perform unauthorized download copy, retrieve, modify or forward of copyrighted materials using VGIL information systems.
- Users shall not connect to Internet through smart phones unless authorized to do so when on VGIL network
- Use of E-mail or communication facilities not provided or authorized by VGIL is prohibited for any official communication.
- Users shall exercise caution while opening emails received from unknown senders, as they may be phishing mails and have malicious contents.
- Users shall not perform unauthorized disclosure of VGIL data in any medium within or outside VGIL.
- VGIL reserves the right to monitor and access as required all use of VGIL information and information systems.
- Users shall be held liable for any defamatory, obscene, offensive, political, proprietary, copyrighted or libelous content posted or stored by them on or using VGIL resources.
- Users whose employment with VGIL stands terminated are not allowed to retain access or any information / data pertaining to VGIL.
- Users shall not connect non-approved systems / external storage drives into VGIL information systems.
- Users shall not plugin or connect any non-approved devices / systems / any portable devices into VGIL' s Wi-Fi or LAN.
- Users shall not store, maintain or back up VGIL data on any personal / unauthorized email account / computing devices **/** data storages not provided by VGIL for official purpose in any form**,** unless explicitly authorized by the Head of department and Manager – SYSTEMS.
- If there is a business need to copy / transfer corporate information to an external portable storage device, prior approval shall be obtained from Department Head and Information Security Team.
- All corporate information in the device should be encrypted and the device shall not contain any information apart from any business data. VGIL's Information Classification Guidelines shall be applied based on business data.

- Users shall not attempt, initiate or establish any network connections with third parties or resources outside VGIL's corporate network unless explicitly approved by the Information Security Team.
- Users shall not misrepresent, obscure, suppress, or replace their own or another user's identity on any VGIL Information System.
- Users shall promptly accept and install critical security updates, software, anti-virus definitions and operating system patches applied on their machines by VGIL IT Team.
- Users shall not test or attempt to compromise or disable any information security mechanism unless specifically authorized to do so by the SYSTEMS Manager.
- Users shall not divulge or comment on VGIL information in any external / public forums, social media platform, blogs and personal sites in any other form unless approved in writing by VGIL's HR Team / Management Committee.
- Before transferring any Information across to third parties, users shall check with Legal and Information Security team and ensure to abide by all the relevant laws, regulations, and compliance requirements.

9.2 Information Classification

All VGIL users share the responsibility for ensuring VGIL information assets receive an appropriate level of protection by observing the Information Classification standard:

- Information 'owners' shall be responsible for assigning classifications to information assets as per the standard information classification system presented below.
- Where practicable, the information shall be labelled based on the information classification. All VGIL information and all information entrusted to VGIL from third parties falls into one of the four classifications in the table below, presented in order of increasing sensitivity.
- **Confidential** – The information assets which have high confidentiality value belong to this category. Only a limited set of authorized users shall access these information assets. Examples include business strategy and personnel files. Confidential data is typically accessible only to top management.
- **Restricted**– The information assets that contain data pertaining to the needs of a specific department, project team, or business process, belong to this category. Such information assets shall be accessible to members of the concerned department, project, or business process only. Restricted data is typically accessible to middle level management, or as per applicability.
- **Company circulation**– The information assets which can be distributed within all offices of V Guard belong to this category. Examples are office orders and internal circulars.
- **Public** – The information assets which do not have any confidentiality requirement and/or can be disseminated to the general public belong to this category. Examples include last year's annual financial report of V Guard and information displayed on V Guard's website.

9.3 Handling of information

Information is created and stored in many formats on a variety of media. Media shall be anything on which information or data can be recorded or stored and shall include both paper and a various of electronic media. Storage devices shall include but not limited to: computer hard drives, portable hard drives, backup tapes, DVD/CD W/RW, USB storage drives, Cloud Storages, and other Personal Digital Assistants (PDA), cell phone, I pods, MP3 players, digital cameras, fax machines, photo copiers, and other types of portable storage devices like microchips.

Media can be used both to store information and to carry it from one location to another. To protect the information, one must safeguard the media against information disclosure, theft, or damage. Proper media labelling, storage, transport, and disposal are risk mitigation controls. Consideration shall also be given to the nature of the information involved (how sensitive is the data), and the format in which it is held or stored.

This policy details the handling of media including storage, transportation, protection and safeguards, and disposal / destruction of media.

- Formal procedures shall be established to ensure safe handling and security of data on electronic media and print media.
- USB ports and CD writers should be disabled on all end-user machines to prevent copying of VGIL data for unauthorized use. On exceptional approval from HOD – Systems, the media devices might be enabled on the user's systems in case there is a valid business requirement.
- Access to DVD, SD-CARD, USB drives, FTP, SFTP and Cloud Storages shall be granted based on authorization from HOD systems.
- Assets owner should ensure that Media (both electronic and print) shall be protected against misuse through password protection and safe cabinets respectively.
- Media shall be protected from physical damages like fire, moisture and magnetic interference during storage and transportation.
- Formal procedures shall be established for all media (including Information Technology (IT) and non-IT assets) for appropriate maintenance, which helps to ensure its continued availability and integrity.
- A stock or inventory of all the media must be maintained by the department Head
- Media shall be disposed-off securely and safely when no longer required. The contents of the media shall be made irrecoverable, if the media will be no longer used.
- Any IT Asset or media shall be disposed securely in accordance to the E-waste policy.
- Approval for removal of media, destruction / disposal of media shall be sought from Information Security team and Respective Department head and a record of such approvals shall be maintained as audit trail.

10 Access Management

10.1 Access to networks and network services

- Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
- Access Rights will be provided as per VGIL's standard Tool based Change Management Process with approvals. User needs to apply through the tool for any addition or updates in access.

10.2 Access Rights Creation/Modification/Deletion/Review Policy

- User access rights shall be configured based on the business requirements for each user to access IT systems, Applications and Data following the principle of least privilege.
- A role-based usage profile, detailing privileges and access rights, shall be assigned to each user.
- Each user shall be uniquely identified by a User ID. Every User ID shall have a secret password that should follow VGIL's Password guidelines.
- No generic User ID shall be permitted except for service accounts on a specific application.

10.2.1 User Access Creation

- New user access IDs on the VGIL corporate network shall be created only upon the receipt of request from HR . ID creation for access to business applications requires prior approval of the respective business department / application owner.
- The user ID creation and access provisioning shall be executed by the nominated personnel.

10.2.2 User Access Modification

- There shall be a formal process to modify user access based on authorizations from Department Head and Application / Asset owner.
- Based on the request from user along with approval from user's reporting manager and application owner, authorized person will modify the access rights of the user.

10.2.3 User Access Disable, Deletion

- Employee termination - HR department should inform the last working date of the employee to SYSTEMS and Information Security team. Application's Administrator would disable the departed employee's access from business applications.
- There shall be a formal process to periodically review the list of registered users and their privileges, to ensure all unauthorized and dormant user accounts are deleted at the earliest and appropriate access levels are maintained.

10.3 User Access Reviews

- All user access and Privileges allocated shall be periodically reviewed.
- The review of access rights associated with generic user accounts in each application should be performed on a quarterly basis. The systems in-charge should compile a department/function wise list of all active user IDs, capturing the following details, but not limited to, user ID, current access and privilege levels, the number of days since last accessed, etc. This list should be forwarded to the respective department/function HOD. The function/department HOD should verify the continued need for all access rights granted. The systems in-charge should modify the access rights based on the review comments and feedback from the respective HOD.

10.4 Privileged User Access Management

- Privileged access includes providing elevated access rights to users for applications, domain, servers, database, network devices and operating systems.
- Privileged access would be provided to authorized users based on their job role, along with the recommendation and approval from the respective department HOD, Manager – Systems and HOD – Systems. Privileged user access shall be restricted to a minimum number of users based on valid business need and reason.
- Privileges associated with each type of operating system, business applications, databases, and network resources shall be identified and managed.
- Privileges shall be allocated to individuals based on the requirements of their job function and role, on authorization from appropriate personnel.
- Privileges allocated shall be periodically reviewed.
- The HOD – Systems should review and verify the continued need for use of all privileged operations granted in the VGIL's IT environment. All changes made to the privilege accounts should be documented and approved. The review of access rights to privileged accounts should be done on a quarterly basis by the HOD – Systems.

- Each administrator should be assigned his/her own unique administrator ID (domain/server/ application/database/network device) to ensure accountability. Administrator IDs will be assigned the necessary administrative capabilities so that the user may carry out his/her assigned job functions.
- Sharing of administrator accounts is not permitted, unless an exceptional approval is obtained from the HOD – Systems and Information Security Head after specifying a valid business justification.

10.5 Remote Access

- VGIL- issued devices shall be authorized to remotely connect to the network. Where non-Organization-issued devices or portals are authorized to remotely connect to the network, appropriate access restrictions should be in place to restrict and secure access.

10.6 Use of secret authentication information

- Employees shall be required to follow the VGIL's practices in the use of secret authentication information.

10.7 Secure log-on procedures and Password management system

- Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure. Password management systems shall be interactive and shall ensure quality passwords.
- Access to information and application system functions shall be restricted in accordance with the access control policy.

10.8 Use of privileged utility programs and Access control to program source code

- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
- Access to program source code shall be restricted.

11 Cryptography

The use of cryptographic controls to secure VGIL' s information shall be based on the results of a formal risk assessment. The output of the risk assessment shall be used to determine the type, strength and quality of the encryption algorithm.

While using cryptographic controls to secure VGIL' s information, the following shall be considered (but not limited to):

- The protection of cryptographic keys;
- Recovery of encrypted information in the case of lost, compromised or damaged keys;
- The impact of using encrypted information on controls that rely on content inspection.

11.1 Encryption

Type and strength of the encryption algorithm shall be decided based on the criticality of the business information handled. The length of the cryptographic key shall comply with contractual requirements and other regulations.

Wherever possible encryption key shall not be transmitted over the network. If the key used to govern the encryption process are to be transmitted over the network, it shall be transmitted through secure communication channels.

- Risk assessment shall be carried out to identify the needs, methodology, business areas and usage of cryptography.
- Cryptographic controls may be used to secure information that is classified as confidential or restricted.
- The definition of confidential information shall be based upon the respective asset owner discretion as per the Information classification policy.
- Confidential information such as logs that are not actively used, when stored or transported in computer-readable storage media (such as servers, storage database drives), shall be in encrypted form wherever feasible and applicable.
- Information used to verify the identification of remote terminals shall be appropriately protected. Static or reusable authentication information shall be encrypted during storage and while passing through the network using encryption mechanism.

However, the key management activities shall be handled by the application to support the use of cryptographic techniques.

Data at Rest

VGIL shall adopt best practices to design networks, with appropriate security policies deployed to maintain a highly secure environment. The data relating to each function shall be isolated and stored in separate folders. Access shall be restricted as per VGIL'S access Control Policy.

Data in Transit

VGIL recommends IPSEC VPN Tunnel or SSL VPN encryption technologies for establishing connectivity to Cloud on open internet to ensure accessing of applications in a secure encrypted environment.

11.2 Cryptographic Key Management

Procedures shall be defined to ensure cryptographic keys being used on VGIL are adequately protected against modification, destruction and unauthorized disclosure.

11.3 Regulation of Cryptographic Controls

Legal advice shall be sought by VGIL to ensure compliance with all relevant laws of the land prior to using cryptographic controls (for e.g. encryption, digital certificates etc.) for protecting VGIL' s information.

12 Physical & Environmental Security

12.1 Physical Entry control

- Designated areas containing VGIL's information assets shall be protected by automated physical entry controls to ensure only authorized personnel are allowed access.
- The Organization shall install Closed Circuit Television (CCTV) cameras at critical areas including the main entry and exit areas of VGIL premises and secure / restricted areas as required.
- Voice phone should be positioned in critical data processing facilities like DC/DR etc.
- Reception shall be staffed to restrict access to the facilities only to authorized personnel and to authenticate visitors with suitable means of identification.
- VGIL shall take necessary measures to protect the integrity of the physical access methods.
- Employees shall always visibly display their ID cards when on premises.
- Employees shall not lend their ID card or borrow colleague ID card to again access.
- Reception employees shall take the following actions as appropriate for individuals not visibly displaying their ID passes:
    - Employees without their ID should be issued a temporary ID;

- A visitor / contractor should be issued a visitor ID after obtaining confirmation from the visitor's host; or
- If none of the above apply, the individual should be escorted from the premises by security where available.
- Employees are responsible to ensure they are not tailgated/followed through entry doors.
- Individuals not displaying ID shall not be permitted to work areas/facility unless authorized by department head.

12.2 Movement of assets

- All asset movements done inside VGIL and assets carried out of VGIL shall be duly authorized and tracked.
- Any personal information storage media such as tapes, hard drives shall not be allowed to be brought inside VGIL, unless approved and authorized by VGIL.
- Any Information / IT material movement beyond the normal working hours should be intimated in advance to the Administration and Information Security Department for smooth operations.

12.3 Removal of Assets

- VGIL shall enforce authorization and control procedures that ensure information systems assets such as equipment or software from VGIL are removed for business purpose only. Appropriate level of authorization from business department head and SYSTEMS shall need to be obtained for removing any VGIL property.
- All information system equipment containing storage media shall be checked to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal.

12.4 Equipment Security – Equipment Placement & Protection

- Information processing resources shall be located away from hazardous processes or materials.
- Adequate power supplies and auxiliary power supplies shall be provided to Information Systems.
- Adequate protection and controls shall be provided to information and information processing resources against damage from exposure to water, temperature, smoke, dust, chemicals, electrical supply interference etc.
- The security protection activities specified by the vendor / manufacturer of information systems equipment shall be implemented.
- Physical emergency procedures shall be clearly documented. VGIL personnel shall be trained in appropriate behavior in emergencies.
- Adequate siting and protection of equipment to reduce the risks from environmental hazards and unauthorized access and misuse shall be implemented.
- Data storage shall be protected from power failures where appropriate e.g. UPS. This shall be monitored and tested by the SYSTEMS department with respective Department or Vendor.
- Power and telecommunications cabling shall be protected from interception or damage where possible.
- Equipment shall be maintained in accordance with manufacturer's instructions and or documented procedures to ensure its continued availability and integrity.
- All equipment containing storage media shall be checked to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal.
- Equipment, information or software shall not be taken off-site without prior authorization from VGIL Business Department Head and SYSTEMS Department Head for respective VGIL Department, Location.

12.5 Security of Electronic Equipment

- All the electronic office equipment including faxes, printers, shall be physically secured.
- Access to the electronic equipment shall be restricted only to authorized users and placed in locations that no visitor can gain easy access without notice of the staff.

Security of Information processing equipment Off-Premises

- Information processing equipment and media containing sensitive data shall not be left unattended in public places.
- Off premises computers with VGIL classified information shall be protected with an appropriate form of access protection, e.g. passwords, smart cards, or encryption, to prevent unauthorized access.
- Manufacturers' instructions regarding physical protection of equipment shall be observed.
- Security risks (e.g. damage, theft, eavesdropping) vary considerably between locations and shall be considered in determining the most appropriate security measures.

12.6 Cabling Security

- Power and communication lines servicing VGIL premise shall be underground, where possible, or subject to adequate alternate protection (concealed wiring). Network cabling shall be protected from unauthorized interception or damage.

12.7 Security of Desktops and Network hubs

- Desktops shall be adequately protected from fire, water, and pollution, damage, and power fluctuations.
- Network hubs shall be secured from fire, heat, dust, and water.

12.8 Power Supplies

- An uninterruptible Power Source (UPS) shall be used to support critical business information processing operations. UPS equipment shall be regularly tested according to the manufacturer's recommendations. Computer hardware shall be protected from electrical surges.
- Alternate power supply sources shall be present to ensure a continuous power supply in the absence of primary power sources.

12.9 Media Handling and Security

- Media shall be protected from physical damages like fire, moisture, and magnetic interference.
- All media shall be handled with care and shall be ensured that they are not kept near magnetic material and are not exposed to any extreme heat or pollution.
- A stock or inventory of all the media shall be maintained.
- Media shall be disposed off securely and safely when no longer required as per E-waste policy.
- Special controls shall be adopted, wherever necessary, to protect sensitive information from unauthorized disclosure or modification e.g. use of locked containers, tamper – evident packaging (which reveals any attempt to gain access).

12.10 Clear Desk and Clear Screen Policy

This section is intended to maintain the confidentiality and integrity of information left on unattended desks or devices. These requirements shall be followed by individuals working at VGIL.

- Storage media containing confidential, restricted information shall be securely stored in locked cabinet while not in use.
- Desktop / Laptop shall be enabled with screensaver session enabled with password protection and no sensitive, confidential, restricted information would be made available.
- Desktops/Laptops should not be left unlocked while the user is away.
- Confidential, restricted information shall not be made available on whiteboards, flipcharts, and notice boards, meeting rooms and pantry rooms.
- Confidential, restricted documents shall not be left unattended.

- Hard copy documents shall be securely stored in locked cabinets and disposed when no longer required.
- VGIL's information in hard copy documents shall not be made available for unauthorized access, e.g. left on desks overnight, placed in general waste bins, left on printers, in meeting rooms or in public areas.
- The Business department heads shall monitor compliance with the clear desk process by performing periodic (Half-yearly) walkthrough across the VGIL's office premises for their respective department, location.

13 Operations Management

Operations management is to ensure that the information processing and communications facilities are used and operated in an appropriately defined manner.

13.1 Documented Operating Procedures

- Operating procedures shall be developed and maintained for all IT processes of VGIL. These procedures shall enable the users to execute their day to day activities and tasks as instructed by the management.
- All operational processes shall represent and comply with the content of the documented operating procedures.

The procedures shall specify the instructions for the detailed execution of each job including:

- Processing and handling of information
- Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities
- Support contacts in the event of unexpected operational or technical difficulties
- Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs.
- System restart and recovery procedures for use in the event of system failure.

13.2 Change Management

- Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

13.3 Capacity Management

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance

13.4 Separation of Test and Production Facilities

The Test and Production facilities / environments must be logically separated.

13.5 Anti-Virus Guidelines

- The latest approved Anti-virus programs shall be pushed to all servers, desktop and laptops on regular basis. Information Security team shall approve the anti-virus programs and IT teams shall implement the same.

- Users shall not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise willfully commit fraud and hinder the performance of or access to any VGIL IT assets.
- All systems should undergo a full anti-virus scan at least once a week and on-access scans should perform on all files and processes. Servers in addition to above should also undergo daily "quick" scans.
- Antivirus software and scan settings should not be changed without explicit approval from the Information Security team. IT should consult with the Information Security team and get explicit approvals if and before making any changes. All approvals shall be retained for compliance purposes.
- SYSTEMS teams are responsible for anti-virus servers to get continuously updated with the latest versions of the virus signature file. The laptops, desktops and other servers shall take the update from central management server or from the internet.
- The user / IT Teams should immediately raise a ticket for any virus incident and also inform the Information Security team.
- All servers, desktops and laptops shall have appropriate configurations to protect against active code (e.g. Java, ActiveX) run from un-trusted sites on the Internet.

13.6 Backup Management

- All application and operating systems software, data (including databases), configuration information of application and operating systems, hardware configuration information (where applicable) and log files / logs from various systems that need to be backed up shall be identified and documented. A list of all the data files for critical applications shall be maintained along with a brief description of the contents of those files.
- Frequency of backup, medium of backup, and storage of the backup shall be identified and documented.
- The backup and recovery procedures shall be automated wherever possible using the system features and shall be monitored and tested for recovery regularly.
- The frequency, extent (e.g. full or differential backup) of backup shall reflect VGIL'S internal requirements, the security requirements of the information involved, and the criticality of the information to the continued operation of VGIL.
- Backup records shall be maintained by personnel and be updated regularly to keep track of the data that has been backed up as well as to control the activity.
- Physical access to the backup copies shall be restricted. Access shall be provided only on a need basis and only upon approval from the SYSTEMS Department Head.
- Additionally, cryptographic controls like encryption may be implemented to ensure safety of critical and highly confidential data backed up.
- The number of backup sets to be maintained shall be decided based on the criticality of information to be backed up.
- In addition to the scheduled backups, backups shall be taken in case any of the following event occurs
- Configuration change
- Upgrade of an operational system
- Back-up media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary.
- The retention period for backup shall be charted out and shall be approved by the SYSTEMS Department Head.
- All movement of tapes between offsite and onsite locations shall be tracked and recorded.
- Periodic audits of backup copies and storage locations shall be carried out.

Recovery

Backed up data shall be provided for restoration purposes after authorization from respective Application Owner(s) and Systems Department Head. Accurate and complete records of the backup copies and documented restoration procedures shall be maintained.

Restoration

- To verify the readability of backup media, mock restoration tests shall be carried out, on the test systems / test environment quarterly with Systems Department Head Approval.
- The entire test process shall be documented detailing the test plan, the activities carried out and the test results.
- Exceptions identified during the testing process shall be documented and reported.

13.7 Logging and Monitoring

VGIL information systems, logs shall be monitored by Systems Technical Team and information security events shall be recorded. Operator logs and fault logging should be used to identify information system problems.

Audit logging

- Information systems that process, transmit, or store sensitive VGIL information shall generate logging data, where such system logging is available and practical.
- Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
- Procedures shall be implemented for monitoring system use to ensure that users are only performing processes that have been explicitly authorized.
- All log data shall be reviewed on a regular basis and exceptions shall be brought to the notice of the management.
- All logs shall be retained as per the agreed retention period.

System monitoring

- Systems shall be monitored, and information security events shall be recorded.
- Critical systems shall be monitored to ensure conformity to access management policy and standards.
- Monitoring of system use shall be in line with the various policies and procedures that are part of the Information Security Management System and any other critical activities.
- VGIL shall have the authority to monitor network traffic, and the employees of VGIL shall be advised that they shall have no expectation of privacy about the use of VGIL network.
- VGIL shall comply with all relevant legal requirements applicable to its monitoring activities.

Log Management

- Logging facilities and log information shall be protected against tampering and unauthorized access to ensure integrity and confidentiality.

- Log information shall be stored securely in line with information classification guidelines to prevent tampering.
- Audit logs shall be archived as part of the record retention policy as evidence for compliance and audit purpose.
- Operator logs and fault logging shall be enabled for identification of information system problems. Such logs shall be reviewed on a monthly basis and appropriate action shall be taken based on the review.
- The clocks of all relevant VGIL information processing systems shall be synchronized with an agreed accurate time source. The correct interpretation of the date/time format is important to ensure that the timestamp reflects the real date/time.

13.8 Vulnerability Management

VGIL' s IT Infrastructure and critical business applications shall undergo periodic vulnerability assessments and penetration testing to identify and mitigate vulnerabilities.

- All applications should undergo a penetration test and all Critical and High rated issues should be remediated before going live.
- All existing systems will undergo periodic assessments and remediation of vulnerabilities as per details outlined in the Vulnerability Management Procedure.
- The identified vulnerabilities shall be classified according to the defined classifications and remediated within the stipulated time frame predefined for each classification.

Examples of vulnerabilities that can be detected using automated tools are;

- Abnormal ownership of directories and files,
- Abnormal permission settings on directories and files,
- Passwords that can be cracked using password sniffers and crackers,
- Poorly implemented / configured Information Security Policy,
- Incorrectly configured network services,
- Well-known system bugs that could be exploited, and
- Unauthorized changes to system files.

14 Communications Security

Communications Security is to ensure that the information processing and communications facilities are used and operated in an appropriately defined manner.

14.1 Network Control

- All network equipment and communication lines shall be identified, documented, and shall be regularly updated.
- Network diagrams at all levels (WAN, LAN, & Segments) shall be maintained and updated regularly.
- Minimum Baseline Security Standards (MBSS) shall be developed and maintained.
- All network equipment shall be configured as per MBSS.
- All network services that are not required on the servers shall be disabled.
- Any problems with the network equipment leading to delay or stopping of any business processes shall be escalated as an Incident.

- NTP (Network Time Protocol) time synchronization shall be implemented across all network devices and servers. All network devices and domain controller shall synchronize with the NTP server. All servers and workstations shall synchronize time settings with the Domain Controller.
- All key network activities should be monitored by Network Team on a periodic basis to assess the performance of the network, reduce the likelihood of network overload and detect potential or actual malicious intrusions. The reports should be examined to discover any unusual use of the network by SYSTEMS Department Head.
- Groups of information services, users and information systems shall be segregated on networks.
- Formal transfer procedures and controls shall be in place to protect the transfer of information using all types of communication facilities.
- Information involved in electronic messaging shall be appropriately protected.
- Requirements for confidentiality or non-disclosure agreements reflecting the VGIL's needs for the protection of information shall be identified, regularly reviewed and documented.

14.2 Limitation of Connection Time

Connection time to the network devices shall be defined. The network devices shall be configured to disconnect automatically after a specified amount of idle time.

14.3 Email Security Policy

Email is a business communication tool and users shall use this tool in a responsible, effective and lawful manner. Guidelines have been detailed out in the Email Security procedure document.

15 Software acquisition, development and Maintenance

15.1 Security Requirement Analysis

- Information systems security requirements shall:
  - Be based on the output from a risk assessment to be performed as a part of project planning / Initiation phase;
  - Reflect the business value of the information assets involved and potential impact of a compromise in confidentiality, integrity and availability of these information assets;
  - Include both automated security controls to be incorporated in the systems and supporting manual controls designed to reduce the risks of security compromise;
  - Comply with relevant legal, contractual and any other requirements, if any.

- Once the security requirements have been defined, modifications to the system's proposed configuration, functionality and information assets shall be accompanied by a review and re-definition, as necessary, of the security requirements. The relevant application security team would assess and provide confirmation on the requirements specification process and if meets the required security standards defined within VGIL.

- Security specifications for the new software shall be documented to provide the development group with specific requirements. This enables VGIL in identifying, reviewing and testing the security functionalities of the software.
- System and physical architecture, interfaces, manual processes and documentation with respect to design phase shall be documented.

15.2 Securing Application Services

- Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

- Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

15.3 Secure development policy

Rules for the development of software and systems shall be established and applied to developments within the organization.

15.4 System Change Control Process

- All changes to applications and software packages shall be:
  - Subject to formal change control process to control and log the changes;
  - Panned and applied only at suitable time except in the event of an emergency;
  - Applied by authorized and experienced personnel only;
  - A fallback/contingency plan that enables a safe return to the original version should be necessary.

15.5 Technical review after operating platform changes

- When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

15.6 Restriction on changes to software packages

- Computer desktops / laptops and printers must not be left logged on, when unattended. Key locks, power-on and screensaver passwords, or other controls shall be used to protect them when not in use.
- As far as possible and practicable vendor supplied software packages shall not be modified.
- If changes are essential, then the original software shall be retained, and the changes shall be applied to a clearly identified copy. While executing the changes, care should be taken to avoid the possibility of compromising the built-in controls.
- Where it is deemed essential to customize vendor supplied software package, the following points should be considered:
- An assessment of built-in controls and integrity processes, which may be compromised due to the changes, shall be made.
- Consent of the vendor for the modifications should be obtained wherever possible.
- Impact on the future maintenance and warranties of the software as a result of changes and modifications should be assessed.
- All changes shall be fully tested and documented, so that they can be reapplied if necessary, to future software upgrades.

15.7 Secure system engineering principles

- Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

15.8 Secure development environment

- VGIL shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

15.9Outsourced development

- Where software development is outsourced, it shall be monitored and supervised. Wherever possible the following aspects shall be considered while outsourcing development:
  - Licensing arrangements, code ownership and intellectual property rights;
  - Certification of the quality and accuracy of the work carried out;
  - Rights of access for audit of the quality and accuracy of work done;
  - Contractual requirements for quality of code;
  - Testing before installation to detect back-doors or Trojan code.

15.10 System security testing

- Testing of security functionality shall be carried out during development.

15.11 System acceptance testing

- Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

15.12 Protection of System Test Data

- The type of data to be used for testing purposes shall be determined and authorized by relevant information asset owners.
- It shall be ensured that if live operational data is used for testing then the data shall be sanitized, and adequate controls should be in place to protect the data.
- The use of operational information containing sensitive customer information or confidential information shall be avoided.
- The use of operational databases containing personal information shall be avoided. Such information if used shall be erased from the test application immediately after testing is completed. Any such use of operational data shall be logged to provide an audit trail.
- Test data shall be removed from test systems when no longer required.

15.13 Software Application Acquisition (Ready to Use / Procure and Customise) at On-premises or On-Cloud or SaaS model

- Software Application / Hosted environment related Assessment Report to be submitted
- VGIL can have Assessment and if found any risks, vendor need to address without any efforts.

15.14 Pre-Implementation Audit for New Developments / Acquisitions

- Internal Audit Team / 3rd party Team to conduct the audit
- If any gaps identified, those must be fixed before go live with audited team's confirmation
- Audit Areas: SDLC, Documentation, BRD v/s developed application

16 Third Party Management

The objective is to provide the third party with an approach and direction for implementing information security controls for all information assets used by them to provide services to VGIL.

- The Third Party shall not process or use VGIL information for any purpose other than the agreed Services and will deliver its services in accordance with the contract.
- The Third party should assign an individual or team who will be responsible and accountable for information security policy implementation and processes and would be acting as the single point of contact for VGIL for information security aspects.
- The Third Party shall establish security controls to prevent accidental, deliberate or unauthorized disclosure, access, or destruction of VGIL information in possession.
- The third party shall ensure all their employees receive formal information security awareness training.

- Disciplinary process for information security breaches shall be established, documented and communicated to the third-party employees.
- Adequate security measures shall be in place when third party employees undergo role transformation within the organization.
- Vendor employees who resign from their organization shall return all assets in their possession upon termination of employment and the access rights shall be revoked or changed appropriately.
- All third parties acting on behalf of VGIL and representatives who are granted authorized access to VGIL and its information assets must comply with the information security policies of VGIL.
- VGIL shall regularly monitor, review and audit supplier service delivery. Changes to the supplier services shall be managed by taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
- All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate VGIL's information or provide infrastructure components.

17 Security Incident Management

A security event is a change in the operations of a network or information technology service indicating a security breach or violation of information security policy but not limited to security incidents in the occurrence of below scenario

  - Loss of sensitive / confidential information
  - Unauthorized access to information
  - Disruption of services
  - Misuse of information and computing resources
  - Incidents related to physical security breaches such as but not limited to, IT Asset lost / stolen, unauthorized entry into premises, physical attack etc.

- Procedures shall be developed for reporting, recording, and investigating and closure of incidents.
- Users shall be educated to recognize a security incident, and immediately report any suspected security indents to infosec@vguard.in They should also notify their manager, Department Head, SYSTEMS Department Head and Information security Head as appropriate.
- Information security team shall perform initial assessment and shall create a ticket in a Ticket Management System capturing the event description, date, source, and rating.
- The Information Security team upon resolving the security incident captures the resolution & the problem category in the ticket and submits it for closure.
- The submitted shall be notified on the incident response. They can verify the response and escalate the ticket if required.
- Users will be involved in the investigation of incidents as and when required. Users shall be informed about the implementation of recommendations made as part of incident response and resolution wherever necessary.
- Emergency response shall be initiated based on escalated information security event and the same shall be declared by the Information Security team.
- All critical incidents and repeated incidents should go through a detailed Root Cause and Corrective Action process (RCCA) involving relevant parties and teams. Learnings from the RCCA activities shall be documented and communicated to all relevant parties. Action need to be taken to mitigate the vulnerabilities and weakness in the system to prevent future incidents.

The detailed procedural guidance on incident handling can be found in the Security Incident Management Procedure.

18 Business Continuity Management

The appropriate level of Business continuity must be ensured so that business processes can be restored when a disruption in assets occurs e.g. due to technical bugs, failure of components, failure of essential services, loss of personnel, or major disasters like earthquakes, fire or floods and including information security in the business continuity management process will be an intrinsic part of the plan.

It is recommended to have a comprehensive risk assessment and business impact analysis at least yearly for key locations, business applications and information assets. These areas should have associated disaster recovery and business continuity plans to minimize impact to service and duration of disruption processes in the event of damage, failure, corruption, lack of availability or loss.

IT Disaster recovery is a subset of VGIL' s overall Business Continuity Management plan. A disaster can be caused by man or nature and which results in the critical facilities and/or information assets and systems not being accessible or functional.

The IT Disaster Recovery Team must identify critical business applications and information assets including computing assets like laptops and desktops of senior management and develop a disaster recovery plan for these.

At VGIL, the declaration of disaster and invocation of the Disaster recovery plan can be made only if at least two of the following persons agree to classify the event as such:

- COO
- CFO
- CIO
- CISO
- Management Committee Members

Disaster Recovery and Business Continuity plans should be tested on yearly basis. Asset owners shall ensure that their assets are suitably protected and covered with appropriate DR & BC Plans. The highest priority in all DR plans shall be given to the protection of human life. The Disaster Recovery Plan, at a minimum, must include the following:

- Criteria to activate the plan including detection of a disaster.
- Escalation guidelines
- Procedure to implement the recovery strategies.
- Recovery Time Objectives
- Recovery Point Objectives
- Responsibility Matrix
- Procedures to revert to normal operations
- Test and Maintenance procedures
- Contact Lists

VGIL employees, contractors and third parties should be aware of their roles and responsibilities in the continuity and recovery plans. They must be aware of critical information such as contact information of key continuity and recovery personnel, call trees (if applicable), and the specific procedures they have to follow.

This ensures VGIL's approach to compliance is consistent and comprehensive having particular regard to:

- Regulatory compliance,
- Legislative compliance,
- Contractual compliance, and

- Policy compliance (both internal and external).

VGIL shall ensure that all its employees and business operations comply with rules, regulations, customs, and practices of the organization.

Crisis Management team and Incident response team shall work collaboratively in the event of a crisis.

19 Compliance

19.1 Compliance with Legal Requirements

- Compliance lead and legal team shall be responsible for any regulatory and legal compliance at VGIL including but not limited to information security related aspects.
- All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
- The business owners shall provide appropriate support to meet the legal requirements with respect to the services rendered at VGIL.

19.2 Intellectual Property Rights

- Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
- Procedures shall be put in place to manage the licenses of software used at VGIL.
- The Departmental Head, Information security team and SYSTEMS department shall then ensure that they define the specific controls, countermeasures and individual responsibilities needed to meet these requirements under the guidance of the Compliance Lead.

Proprietary software products shall be normally subject to licensing agreement. Use of the software may be limited by number of machines, users or by site. The following requirements shall be adhered to:

- No copyrighted material shall be copied without the copyright owner's written consent.
- Users shall not copy software from one machine to another without the asset owner's documented authority.
- Copying or using proprietary or organizational software on computers that do not belong to VGIL shall only be carried out with written consent from the User Department Head, SYSTEMS Department Head and Compliance Head or CFO.
- Where it shall be necessary to use a software product on additional machines, licenses shall be extended, or additional copies purchased before software shall be installed on extra computers.
- Employee should use the IT assets (products, software, information) covered by intellectual property rights in line with legislative, regulatory and contractual requirements.
- Employee should accept that all intellectual property produced, created, compiled, devised or brought into VGIL during employment is the property of VGIL and should be protected.

The SYSTEMS department shall conduct audits of software use, maintain software registers, and delete unauthorized software products on a quarterly basis. Copyright infringements shall lead to legal action, and possibly criminal proceedings.

19.3 Protection of Records

- Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.
- VGIL's legally binding or statutory information shall be protected from loss, destruction, falsification or breach of confidentiality.
- Retention of records shall be required to meet statutory requirements or to support business critical activities / departments. Records shall be required to demonstrate that VGIL operates within statutory regulations and have appropriate controls in place to protect against potential civil or criminal suits or that shall establish the financial status of VGIL.
- The records shall be provided with adequate amount of protection based on the relevance, classification, and importance of the records, and shall be stored in a manner appropriate to the media on which they shall be recorded.

19.4 Privacy and protection of personally identifiable information

- Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
- The Legal and Compliance Head shall be responsible for identification and implementation of appropriate controls for privacy and protection of personally identifiable information.

19.5 Regulation of cryptographic controls

- Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

19.6 Independent review of information security

- The organization's approach to manage information security and its implementation shall be reviewed independently at planned intervals or when significant changes occur.
- Information processing resources and associated documentation shall be reviewed immediately after installation and thereafter on a yearly basis to verify that they are compliant with the documentation developed. Findings and recommendations in the report shall be communicated to the concerned department personnel for implementation and to the Department Head for tracking to closure.
- VGIL's information processing resources shall be reviewed by an independent third party on an annual basis. The findings shall be reported to VGIL's Senior management.

19.7 Compliance with Security Policy

- Department responsible for implementation of ISMS policies and procedures shall ensure that all the designated personnel for execution understand and comply with the policies and procedures.

19.8 Technical compliance review

- Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

20 Exceptions

This Procedure is intended to address Information Security requirements. Requested waivers shall be formally submitted to Management Committee of VGIL including justification and benefits attributed to the waiver for approval. The waiver shall only be used in exceptional situations (subject to a maximum period of 60 days). At the time of completion, the need for the waiver shall be reassessed and re-approved, if necessary. Waiver

shall not be provided for more than three consecutive terms. The waiver shall be monitored to help ensure its concurrence with the specified period and exception.

21 Reference Procedures

- VGIL – ISMS Internal audit management review and compliance procedure
- VGIL – ISMS Business continuity management procedure
- VGIL – ISMS ITSM procedure
- VGIL – ISMS Asset Management Procedure
- VGIL – ISMS Access Management Procedure
- VGIL – ISMS Risk management procedure
- VGIL – ISMS Media handling procedure
- VGIL – ISMS Vendor management procedure
- VGIL – ISMS Information classification, labelling and handling procedure
- VGIL – ISMS Backup and restoration procedure
- VGIL – ISMS Vulnerability management procedure
- VGIL – ISMS HR Security Procedure
- VGIL – ISMS Email Security Procedure
- VGIL – ISMS Mobile Remote and teleworking procedure

22 ISO References

- ISO 27001: 2013 - A.8.2.1 Classification of information
- ISO 27001: 2013 - A.8.1.3 Acceptable use of Assets
- ISO 27001: 2013 - A.8.1.4 Return of Assets
- ISO 27001: 2013 - A.8.2.2 Information Labelling and handling
- ISO 27001: 2013 - A.8.2.3 Handling of Assets
- ISO 27001: 2013 - A.7.2.3 Disciplinary Process
- ISO 27001: 2013 - A.12.6.1 Management of Technical vulnerabilities
- ISO 27001: 2013 – A 15.1. 1 Information Security Policy for Supplier Relationships.
- ISO 27001: 2013 – A 15.1. 2 Addressing Security Within Supplier Agreements.
- ISO 27001: 2013 – A 15.1. 3 Information & Communication Technology Supply Chain.
- ISO 27001: 2013 – A 15.2. 1 Monitoring & Review of Supplier Services.
- ISO 27001: 2013 – A 15.2. 2 Managing Changes to Supplier Services.
- ISO 27001: 2013 – A 7.1.2 Terms and Conditions of Employment
- ISO 27001: 2013 - A.18.1.4 Privacy and protection of personally identifiable information
- ISO 27001:2013 - A.12.2.1 Control Against Malware
- ISO 27001: 2013 – A.9.3.1 – Use of secret authentication information
- ISO 27001: 2013 – A.12.4.1 Event logging
- ISO 27001: 2013 – A.12.4.2 Protection of log information
- ISO 27001: 2013 – A.14.4.3 - Administrator and operator logs
- ISO 27001: 2013 – A.14.4.4 - Clock Synchronization
- ISO 27001: 2013 - A.7.1.2 Terms and conditions of Employment
- ISO 27001: 2013 - A.7.1.1 Screening
- ISO 27001: 2013 - A.7.2.1 Management responsibilities
- ISO 27001: 2013 - A.7.2.2 Information security awareness, training and education
- ISO 27001: 2013 - A.7.3.1 Termination or change of employment responsibilities
- ISO 27001: 2013 - A.7.2.3 Disciplinary Process
- ISO 27001:2013 - A.6.2.1 Mobile Devices Policy
- ISO 27001:2013 - A.6.2.2 Teleworking
- ISO 27001:2013 - A 8.1.3 Acceptable use of assets
- ISO 27001:2013 - A 8.2.3 Handling of assets
- ISO 27001: 2013 - A17.2.1 – Availability of information processing facilities

- ISO 27001: 2013 – A.12.3.1 Information Backup.
- ISO 27001: 2013 – A.12.2.1 Controls against malware
- ISO 27001: 2013 – A.14.2.3 - Technical review of applications after operating platform changes