Information Security Policy Manual

KG Invicta Services (KGiS)

[Ref: ISM-PLC-DOC-01]
[Ver: 0.1]
[05th December 2022]
[Classification: Internal]

+91 422 4419999

KGiS
o 365, KG Invicta Services Private Limited KGiSL Campus, Thudiyalur Road, Saravanampatti, Coimbatore - 641035, India

www.kginvicta.com

Statement of Confidentiality

This document contains confidential and proprietary information of KG Invicta Services Private Limited (KGiS). It is furnished for KGiS internal use and purpose only. Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose. This document is reviewed at least annually.

Copyright and Intellectual Property

Table of Contents

1 Document Control

1.1 Document Owner and Approval

KGiS's Information Security Office (ISO) is the accountable owner of this policy. The ISO is responsible for ensuring that this document is reviewed periodically by the relevant stakeholders in line with the review requirements of the Information Security Management System (ISMS).

A current version of this document is available to all KGiS members at the corporate Intranet and is published on 05 Dec 2022.

This policy document was approved by the Senior Management on 05 Dec 2022, and the KGiS CEO on 05 Dec 2022 and met the required Documentation Quality Standard and is issued on a version-controlled basis under the signature.

Name: Shanmugam C

Designation: GM - ICT

Signature: Date:

1.2 Amendment History Record

Version	Description of Change / Action	Resource	Date
1.a	New draft baseline of ISMS policies	Harikrishnan P	04-Dec-2022
1.0	Verified and Approved By	Shanmugam Chinnasamy	05-Dec-2022

1.3 Cross References

All reference documents available in – Shared Folder
ISO 27001– Information technology – Security Techniques – Information security – Requirements
ISO 27002 – Information technology – Security techniques – Code of practice
ISO 22301 – Business Continuity Management System (BCMS) Policy

1.4 Document Sign off and Distribution

Name	Designation	Signature	Version	Date
	Chief Executive Officer		1.0	

Document Distributed for Internal Approval.

Stakeholder	Date
All Head of Departments and Departments	

2 Glossary

Term	Definition
ActiveX	ActiveX is a technology developed by Microsoft. With an ActiveX-enabled browser (i.e., Internet Explorer only) ActiveX controls can be downloaded
Adware	Adware or advertising-supported software is any software package which automatically plays, displays, or downloads advertisements to a computer
Alphanumeric	Consisting of letters and numbers, especially the characters A to Z (lowercase and uppercase) and 0 to 9;
Archiving	The process of saving emails for later reference or use.
Attachment	An e-mail attachment is a computer file which is sent along with an e-mail message.
Availability	Availability relates to information being available when required by the business process both now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
Bulletin Board	A computer that is running software that allows users to leave messages and access information of general interest
Case sensitive	Distinguishing upper- and lower-case letters
Chat Rooms	A public forum on the internet where information, views, etc. can be exchanged
Confidentiality	Confidentiality concerns with the protection of sensitive information from unauthorized disclosure.
Cookies	A cookie (also tracking cookie, browser cookie, and HTTP cookie) is a small piece of text stored on a user's computer by a web browser
Email Client	An application program used to receive, store and send email
Firewall	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.
IDS	Intrusion Detection System
IMAP	The Internet Message Access Protocol (IMAP) is one of the two most prevalent Internet standard protocols for e-mail retrieval
Information Asset	Following are examples of various types of Information Assets: a) **Information:** databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fall-back arrangements, audit trails and archived information Software Assets: application software, system software, development tools, and utilities b) **Physical assets:** computer equipment, communications equipment, removable media, and other equipment c) **Services/Processes:** computing and communications services, general utilities, e.g., heating, lighting, power and air-conditioning d) **People**: qualifications, skills, and experience
Integrity	Integrity is related to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
Interested parties	Employees, Partners, Contractors, Customers, Stakeholders and Third-Party organizations delivering services to KGiS
Intellectual Property	Any product of someone's intellect that has commercial value, including copyright material, patents, trademarks and know-how or confidential information.
IPS	Intrusion Prevention System

Term	Definition
JavaScript	A scripting programming language most commonly used to add interactive features to Webpages
Journaling	A journaling file system is a file system that logs changes to a journal
Malicious Software	Malicious Software includes Virus, Malware, Adware, and Spyware programs that may cause serious damage to the computer system, network and data.
Malware	Software designed to infiltrate or damage a computer system without the owner's informed consent.
Masked	Used to disguise an entry into a workstation to keep the entry confidential.
Password	A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource
Patches	A patch is a piece of software designed to fix problems with, or update a computer program or its supporting data
Proxy	A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing
Public Forum	An internet forum that is open to public expression.
Removable Storage Media	Storage media which is designed to be removed from the computer without powering off the computer. Examples include Memory Cards (memory stick, digital card), Magnetic Tapes, USB Flash Drives, External Hard Disk Drives
Sensitive Document	Documents comprising of information or knowledge that might result in loss of an advantage or level of security if disclosed to others who might have low or unknown trust ability or undesirable intentions.
SMTP	Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks
Spyware	Computer software that obtains information from a User's computer without the User's knowledge or consent
Stakeholder	KGiS Executive Management and Board Members as well as all KGiS Staff Members and short-term employment contractors or any person or entity working or interacting with KGiS on any level providing a service or other beneficial action within the confines of KGiS's corporate domain.
Super User	Administrator User or a User who can assign privileges to other Users.
Trojan	A program that appears desirable function for a user but instead facilitates unauthorized access to the user's computer system
User Id	A User ID uniquely identifies an individual on a computer or other network device.
Users	Authorized employees, partners, third parties and anyone accessing and using the Information and Information systems
Virus	A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer
Web Messenger	Form of real-time communication between two or more people based on typed text
Web Page	A document connected to the World Wide Web and viewable by anyone connected to the internet who has a web browser
Worm	A software program capable of reproducing itself that can spread from one computer to the next over a network

3 Acronyms

Acronym	Abbreviation
Datacenter	KGiS Data Center
ISMS	Information Security Management System
ISO	Information Security Office
RA	Risk Assessment
BIA	Business Impact Analysis
SoD	Segregation of Duties
HR	Human Resources
HRMS	Human Resource Management System
BYOD	Bring Your Own Device
POD	Personal Owned Devices
NDA	Non-Disclosure Agreement
ITO	Information Technology Office
SLA	Service Level Agreements
SOC	Security Operations Centre
ISRM	Information Security Risk Management
C&L	Contract and Legal
DMZ	De-militarized Zone
DLP	Data Leakage Prevention
MoU	Memoranda of Understanding
ISIRT	Information Security Incident Response Team
SIM	Security Incident Management
BCM	Business Continuity Management Program
RTO	Recovery Time Objective
RPO	Recovery Point Objective
DRP	Disaster Recovery Plan
DRS	Disaster Recovery Site
BCP	Business Continuity Plan
CIP	Continual Improvement Plan
MSB	Minimum Security Baseline
SIEM	Security Incident Event Management
EDR	Endpoint Detection and Response
SOC	Security Operation Center
BCM	Business Continuity Management
DKM	Domain Keys Identified mail
SPF	Sender Policy Framework
DMARC	Domain based message authentication, reporting and conformance

4 Introduction

4.1 Overview

KG Invicta Services Private Limited (KGiS) is a leading Business Process Management (BPM) solution provider focused on maximizing the efficiency of organizations and enabling them to do impactful work. KGiS take care of your crucial business processes so that you can focus on your core expertise, boost your productivity, and make better decisions to achieve your goals. KGiS bring in top talents, futuristic technology, and effective strategies to deliver incremental business value that contributes to exponential growth.

KGiS helping clients around the world, from locations on-shore and offshore, with various business processes including customer engagement, talent acquisition, finance and accounting, and back-office processes. Our services are tailored to increase your capabilities, alleviate operational setbacks and help you realize your vision.

KGiS is committed to Information Security to deliver its services and to continually improve its posture as part of its Information Security Management practices. This revised version of the Information Security Policy aims to encompass all the Information Security directives and statements in a single document to ensure effective maintenance, review and approval timeframes.

4.2 Purpose

The purpose of this policy is to provide a clear, structured and exhaustive set of guidelines to help KGiS personnel and other key interested parties apply adequate Information Security Management practices, demonstrates the management's commitment and emphasis towards Information Security.

The policy provides management's direction to safeguard the Confidentiality, Integrity, and Availability of Information Assets (i.e., Information and Information Systems) from all threats and vulnerabilities, internal or external and deliberate or accidental, thereby ensuring uninterrupted services to interested parties.

The policy also guides on how to manage risks to an acceptable level through design, implementation and maintenance of an effective Information Security Management System (ISMS) and meet the requirements established in the ISO 27001:2013 Information Security Standard, PCI-DSS, SOC and other relevant requirements from the stakeholders.

Finally, this Policy forms the baseline and identifies key principles for all Information Security initiatives in KGiS.

4.3 Key Objectives

KGiS information assets shall be adequately protected from threats and vulnerabilities to safeguard its Confidentiality, Integrity, and Availability. This Information Security policy supports the creation of a secure business environment by establishing overall direction and key principles, developing awareness and imparting education to all interested parties.

4.4 Scope & Applicability

The scope of the policy covers all products and services provided to KGiS and its clients as applicable.

4.5 Compliance & Enforcement

Compliance to the Policy statements and principles defined in this document is 'Mandatory' for all interested parties involved in the management, operations, administration, and third parties. The Policy and principles defined in this document shall be enforced by the Information Security office (ISO). Any exceptions to the defined controls in this policy shall be exclusively approved by KGiS Information Security Office.

ISO shall ensure that audit records for Information Systems are regularly reviewed and analysed for indications of inappropriate or unusual activity. Any suspicious activity or suspected violations are investigated, and findings are reported through appropriate channel to take necessary actions.

Hence, violations of the Policy statements may result in disciplinary action, including dismissal and legal action against the offending Employee(s), Contractors, and Third-Party organization, consistent with law or contract terms as applicable.

4.6 Policy Statement Terminology

Term	Description
SHALL	This word, or the terms "**MANDATORY**", "**REQUIRED**", "**WILL**" or "**MUST**", means that the definition is an absolute control requirement of the applicable standard or specification.
SHALL NOT	This phrase, or the phrase "**MUST NOT**" or **"WILL NOT"**, means that is an absolute prohibition of the applicable standard or specification.
SHOULD	This word, or the adjective "**RECOMMENDED**", means that there may exist valid reasons circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "**NOT RECOMMENDED**" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective "**SUGGESTED**" or "**OPTIONAL**", means that an item is truly optional.

5 Information Security Policy

5.1 Objective

To provide management direction and support for information security in accordance with KGiS business requirements and relevant India laws, standards, and regulations.

5.2 Information Security Policy Statement

"KGiS shall ensure confidentiality, integrity, and availability of its information systems and the information processed, stored, and transmitted by those systems to establish a trusted, reliable and secure business environment by implementing appropriate information security controls."

5.3 Information Security Policy Structure

The KGiS's ISMS policy is structured in a manner that conforms to the management and functional areas of ISO 27001/2:2013 International Standard and Code of Practice, the management and technical controls of Global Cyber Security Standards, considering the areas specific and pertinent to KGiS.

These areas include the following and as depicted below:

a. Information Security Policy;

b. Organization of Information Security;

c. Human Resource Security;

d. Information and Asset Management;

e. Identity and Access Management;

f. Cryptography;

g. Physical & Environmental Security;

h. Operations Security;

i. Communications Security;

j. System Acquisition, Development and Maintenance;

k. Supplier Relationship;

l. Information Security Incident Management;

m. Information Security aspects of Business Continuity Management; and

n. Compliance.

5.4 Review Period

To ensure the policy's continued suitability, adequacy and effectiveness, the information security policy statements in this document shall be reviewed and updated at planned intervals (at least

annually) or if significant changes occur to the organizational environment, business circumstances, legal conditions, and / or technical environment.

5.5 Supporting Policy Statements

The following pages and sections contain the policy statements supporting the main overarching statement above.

6 Organization of Information Security

6.1 Objective

To establish a management framework to initiate and control the implementation and operation of information security within KGiS.

6.2 Policy Area: Information Security Governance

6.2.1 Policy Section: Information Security Internal Organization and Planning

1. KGiS shall appoint an 'ISO' responsible for leading and managing all Information Security activities.
2. KGiS shall ensure that the ISO and the team are appropriately qualified and maintain the required Information Security qualifications and competence in line with their job and applicable standards for Information Security.
3. KGiS shall establish an Information Security Steering Committee (ISSC) with representatives from both the Executive Management, Contracts and Legal and Information Technology Management sections to supervise the application of the Information Security Policy and convey KGiS Executive Leadership commitment towards effective Information Security Management.
4. The ISSC shall conduct management reviews on a **Half-Yearly** basis to review effectiveness of ISMS and this shall include: status of actions from previous management review meetings, external and internal changes, feedback on performance, non-conformities and corrective actions, monitoring and measurement, audit results, fulfilment of objectives, feedback from interested parties, results on risk assessments and risk treatment plans, and opportunities for continuous improvement.
5. The results from management reviews shall be documented and the management review minutes record shall be distributed to all review participants.
6. KGiS shall define the roles and responsibilities of the ISO and similarly for other Information Security functional requirements.
7. KGiS shall identify the internal business services/functions and engage with the function heads to facilitate Business Information and Categorization to ensure Confidentiality, Integrity and Availability within functional areas, in line with the Information Classification Management Policy statement in this document.
8. KGiS shall prioritise the business services/functions according to business criticality through Risk Assessment (RA) and a Business Impact Analysis (BIA).
9. KGiS shall define and apply an Information Security Risk Management process that; establishes and maintains risk acceptance criteria and criteria for performing risk assessments as outlined in the Information Security Risk Management Framework.
10. KGiS shall conduct a formal risk assessment process annually incorporating the following actions:

a. Identification and analysis of security risks associated with loss of confidentiality, integrity, and availability'
b. Identification of risk owners;
c. Identification of threats to KGiS Information Assets and business functions;
d. Identify possible vulnerabilities that may be exploited by current threats;
e. Determine possible impact should Confidentiality, Integrity or Availability of Information Assets be compromised;
f. Determine the likelihood of threats;
g. Evaluate existing controls;
h. Calculate residual risk values; and Present residual risk values along with recommended controls to Core Management team and Stakeholders for formal acceptance.

11. KGiS shall document all the results from the formal risk assessment process.
12. KGiS shall define and apply an Information Security Risk Treatment process to select treatment options after obtaining risk owners' approvals on treatments and residual risks.
13. KGiS shall document all information on the risk treatment process.
14. KGiS shall implement appropriate controls as per the risk treatment process document.
15. KGiS shall select and implement security controls considering the legal legislation compliance, Intellectual Property Rights, protection of organization records, protection of privacy of personal Information and prevent misuse of Information Processing Facilities.
16. KGiS shall develop and document an Information Security Management Strategy Framework to ensure that KGiS Information Security requirements are addressed and managed accordingly.
17. KGiS's Internal Audit (IA) shall conduct internal information security audits and the audit program and results shall be documented.
18. KGiS shall act on non-conformities from information security audits, evaluate the need for actions, implement actions and all this information shall be documented.
19. KGiS shall evaluate the ISMS performance and effectiveness and the evidence of monitoring and measuring shall be documented.
20. Information Security Office (ISO) shall evaluate and measure the ISMS performance once in **three** months.
21. KGiS shall continually improve the Information Security Management within KGiS.

6.2.2 Policy Section: Information Security Roles and Responsibilities

1. The KGiS ISO is responsible for establishing, implementing, maintaining, and continually improving the ISMS.
2. The KGiS ISO is responsible for the development, maintenance, and distribution of KGiS Security Policies.

3. The KGiS ISO and internal audit are responsible for self-assessments and audits of compliance to KGiS Information Security Policy.
4. Department Heads and service owners, and their respective champions are responsible for compliance to KGiS Security Policy within their own area(s).
5. All employees, Contractors and Third-Party organizations performing duties for or on behalf of KGiS, are responsible for reading, understanding, acknowledging and complying with KGiS Security Policy.
6. The ISSC and ISO are responsible for the review of KGiS Information Security Policies on a scheduled and on-going basis to ensure its continued suitability, adequacy and effectiveness.

6.2.3 Policy Section: Segregation of Duties (SOD)

1. The organization structure of all Department/Departments shall consider SoD while defining roles and responsibilities of the respective employees.
2. A SoD matrix for every critical Information System (e.g. application, database, operating system, technical solution, network, security, etc.) shall be developed by business/service owner or custodian to indicate the positions where conflict of interest may arise if access of any distinct function is granted to same person / group / department.
3. Role based access to systems shall be granted by ensuring SoD matrix to avoid Conflict of Interest.
4. SoD for different roles shall be ensured during development / testing, implementation and on-going production.
5. Non-production (development / test) and production environments shall be segregated because of the different nature of requirements for Access Control and Confidentiality.
6. In the event where business functions cannot be segregated appropriately due to specific circumstances, management shall evaluate the risk and implement mitigating controls such as monitoring activities, audit trails and management supervision.
7. The SoD with respect to application, database, operating system, technical solution and personnel shall be periodically reviewed by the respective business owners.

6.2.4 Policy Section: Contact with Authorities

ISO in coordination with the Legal Department shall identify and maintain contact lists of authorities/ regulatory bodies such as Civil Defence, Police, Cyber Crime, Security and Forensics Department, Cert Cyber Security Intelligence, etc. to receive updates on new laws and regulation, vulnerabilities and security threats etc.

6.2.5 Policy Section: Contact with Special Interest Groups

1. The ISO shall maintain contacts with the following special interest groups, but not limited to:
    a. **Special Security Forums**: These forums enhance security of Communications and Information infrastructure through proactive action and effective collaboration with

other security bodies. These forums issue security guidelines, advisories, share information relating to latest threat and changes in information security.

b. **Security Advisories:** Security advisories provide objective, timely and comprehensive information about security threats and vulnerabilities. For example, ISP, Stakeholder Security Forums, ISACA, ThreatConnect, Cert etc.

c. **Security Vendor Updates:** Vendors should be contacted for hardware and software updates, patch updates, latest vulnerabilities etc.

6.2.6 Policy Section: Information Security in Project Management

1. KGiS shall address information security in project management, regardless of the type of the project.
2. Information security shall be integrated into KGiS's project management methods to ensure that information security risks are identified at the information gathering stage and addressed in initial phases as part of the project.
3. The project management methods in use should require that:
   a. Information security objectives are included in project management;
   b. An information security risk assessment is conducted at an early stage of the project to identify necessary controls;
   c. Information security is part of all phases of the applied project methodology; and
   d. Assurance on no vulnerability by ensuring Compliance & Security scan before moving to production.
4. KGiS should address and review regularly all information security risk and implications in all projects.
5. KGiS should define and allocate information security roles and responsibilities in the project management methodology.

7 Human Resources Information Security

7.1 Objective

To address the information security requirements of Human Resources (HR) prior to employment, during employment and through termination or change of employment stages.

7.2 Policy Area: Human Resources Security Policy

7.2.1 Policy Section: Job Description

1. General Information Security and Business Continuity responsibilities shall be included in all job descriptions, code of business practice, employment contracts and confidentiality agreements to all interested parties as released by the HR Department of KGiS.
2. A set of rules that describes staff responsibilities and expected behaviours with regard to Information system usage shall be readily available to all interested parties.

7.2.2 Policy Section: Screening

1. The HR shall perform background verification and screening for all employees, contract workers, and third-party employees accessing critical Information systems prior to their employment or engagement period.
2. The screening and background verification shall be conducted by HR staff and must be proportional to the role and responsibilities that a candidate is going to be accountable once employed.
3. The HR shall keep signed employment contracts in original form as acknowledgements that the employee has read, understood, and agreed to abide by their security responsibilities.
4. HR shall periodically review and update the contract.

7.2.3 Policy Section: Terms and conditions of employment

1. Employees, contract workers, and third-party users of KGiS Information processing facilities shall sign and acknowledge respective engagement contracts, which outlines their security roles and responsibilities.
2. The Employee's responsibilities on adherence to legal requirements (e.g., copyright laws or data protection legislation, etc.) shall be included in the terms and conditions of employment.
3. The terms and conditions to be signed by employees should include non-disclosure agreement (NDA) clauses.
4. KGiS shall include all the disciplinary actions to be taken as per "HR Policy", if the employee disregards the KGiS's security requirements in the terms and conditions.

7.2.4 Policy Section: Security during Employment

1. The HR Department shall ensure that employees, contractors, and third-party users are informed and familiarized with KGiS Information Security policies and procedures.

2. KGiS employees shall be given the necessary training and awareness of Information Security policies and procedures, security requirements, business controls, and the correct use of IT facilities owned by KGiS by Information Security Office.
3. Details of the induction and awareness training shall be documented and maintained by HR.
4. Each employee shall be provided with training and awareness sessions regarding Information Security. Additionally, those who are involved with technical security responsibilities shall be provided with additional security education that corresponds to their specific job role and function.
5. Employees shall be trained and are mandated to report suspected security breaches, security weaknesses or security threats on Information Systems or Information Services through management channels as quickly as possible.
6. HR shall securely manage and retain any personnel background reports received from the Tamilnadu Police and / or other security authorities.
7. HR shall implement a formal disciplinary process for employees who have committed a security breach in accordance with KGiS's HR Policy from time to time.
8. Employees shall acknowledge complete understanding of Information Security Policy and their responsibilities of information security towards organization annually.

7.2.5 Policy Section: Management Responsibilities

1. Management shall require all employees to abide with the established policies and procedures of KGiS.
2. Management shall ensure that employees are aware of their information security roles and responsibilities.
3. Management shall ensure that employees conform to the terms and conditions of employment.
4. Management shall ensure that employees are educated or trained regularly on the relevant skills and qualifications.

7.2.6 Policy Section: Information security awareness, education and training

1. The ISO shall identify roles and assign responsibilities for all ISMS functions and activities.
2. Skills and competency requirements including qualification, experience and other special skills required for each role shall be identified and documented by the HR.
3. A comprehensive training and awareness program addressing the requirement, based on the skills gap report, for all ISMS roles shall be formulated.
4. A training plan shall be prepared based on the training and awareness program by Learning and Development.
5. Periodic Information security awareness and education sessions shall be conducted for all KGiS employees to provide an awareness of responsibilities and any changes to the Policy.
6. The awareness sections shall cover Information Security basics, associated policies and procedures, and employee responsibilities.

7. Information Security awareness and education material shall be made available for all employees who have access to KGiS Information Assets.
8. Training and awareness evaluation methods and criteria for measuring of effectiveness of ISMS training will be implemented by HR.
9. Line managers shall nominate and ensure that each team member attends KGiS Security awareness training to improve their knowledge of the Information Security Policy and understanding of their responsibilities to increase employee efficiency and effectiveness towards organizational security.
10. Qualifications prior to joining and whilst employed will be maintained and recorded by Learning and Development.

7.2.7 Policy Section: Disciplinary Process

1. KGiS shall take proper disciplinary actions against employees who have committed an information security breach.
2. KGiS shall conduct investigation after information security breach has occurred.
3. KGiS shall apply disciplinary actions against employees when the impact of breach effects business.
4. KGiS shall apply disciplinary actions to prevent employees from violating the KGiS's information security policies and procedures.

7.2.8 Policy Section: Termination or Change of Employment

1. In case of employee resignation, access from Information Systems shall be suspended effective the last day of service.
2. In case of employee termination, access from Information systems shall be suspended effective the date of issuance of termination order.
3. User IDs suspended due to termination / resignation shall be disabled and moved to "Disabled Organization Unit (OU) on Active Directory.
4. Physical access cards or tokens to KGiS facilities shall be withdrawn and deactivated on the last day of service.
5. All Information assets issued to the concerned employee shall be recovered with immediate effect and prior to settlement of dues and departure from KGiS.
6. All employees shall be interviewed before their departure, and details (e.g., reminder of confidentiality obligations, etc.) of the interview shall be documented for future reference.
7. A complete knowledge transfer along with documented information and communications shall be provided to Line/department manager to ensure business function/service continuity.
8. All access shall be revoked for any termination, resignation and inter department transfers. Any exceptions shall require approvals from Information Security Office.
9. Any Inter-department transfer shall have approvals from Line Manager and Business Head along with skills and expertise to justify the new role.

8 Information and Asset Management

8.1 Objective

To ensure that all KGiS Information and Assets are identified, and appropriate protection responsibilities are defined and applied.

8.2 Policy Area: Information and Asset Management Policy

8.2.1 Policy Section: Inventory of Information and Assets

1. KGiS shall identify all Information and Assets that either directly or indirectly contains, stores or processes Information pertaining to the business of KGiS whether physical or digital.
2. Information Security office (ISO) shall assist Information and Asset Owners (Head of Department who are accountable to ensure security of Information generated, stored or processed within the department) to maintain an Information Asset Register including information name, owner, type, storage medium, category, retention period, Business value, CIA value, etc.
3. Information asset register shall be easily accessible to Information owner to update it on regular basis and Information Security Office shall ensure that the Information Asset Register is accurate and up to date.
4. IT asset register shall be maintained and updated by ICT and shall be provisioned to Information security office as and when required.

8.2.2 Policy Section: Ownership of Assets

1. KGiS shall assign a designated owner for each Information Asset in the Asset Register. The Asset Owner shall:
    a. ensure that vital information regarding the Information is updated and managed appropriately;
    b. ensure clear understanding of Information asset classification policy and appropriately classify assets and ensure the protection controls for the asset;
    c. ensure that Information assets are inventoried;
    d. ensure adequate information security controls are in place during storage and transmission of information asset;
    e. periodically review access and classifications to important assets under his/her ownership; and
    f. ensure proper handling when the asset is deleted or destroyed.

8.2.3 Policy Section: Acceptable Use of KGiS Information Assets

1. Users shall ensure that internal KGiS Information, client Information and / or any other sensitive Information pertaining to KGiS business, obtained in the course of performing his

/ her job function, be kept confidential and shall not be shared with or disclosed to any unauthorized party.

2. Users shall use KGiS Desktops, Laptops, Networks and other Information and Communication resources for legitimate business purposes only.
3. Internet access shall be used to conduct the business of KGiS in an efficient and convenient manner. Incidental personal use is permissible providing individual job performance is not affected as per the discretion of the individual's Line Manager.
4. Users shall wear their Identification cards visibly inside office facility.
5. Users should lock their workstation during breaks/ away from desk.
6. Users should report any suspicious behaviour to KGiS Information Security Office immediately.
7. Users shall report any loss or suspected loss of data to Information to KGiS Information Security Office.
8. Users shall change their password if you have any suspicion that it may have been compromised.
9. Users shall maintain the desk and screen clean as per Clear Desk and Clear Screen Policy.

8.2.4 Policy Section: Unacceptable Use of KGiS Information

1. Use of KGiS Information Assets and Communication Resources without authorization under the Access Control Policy or without explicit authorization from Information Security Office/CISO for non-standard usage which is not already permitted by the Access Control Policy.
2. Wilfully gaining or attempting unauthorized access to restricted data or Information.
3. Logging into a Server / Computer / Account without explicit authorization.
4. Introducing malicious program code, knowingly or unknowingly, onto KGiS Information Assets and Communication Resources.
5. Installing any Software, including utility tools, whether licensed or not, on KGiS Information Assets and Communication resources without proper authorization
6. The disabling of Security Services, Devices or Software on any KGiS Information Asset and Communication Resources unless explicitly authorized by the Information Security Office (ISO).
7. Revealing passwords to others or allowing the use of accounts by others. This includes family and other household members when working at home.
8. Installing or utilizing methods that circumvent the Security Services, Controls and Devices.
9. Disrupting or attempting to disrupt the proper functioning of any Computer Equipment.
10. Breaching or disrupting Network Communications or attempt to do so.
11. Network Monitoring, Port Scanning, Security and Vulnerability Scanning unless authorized by the ISO.

12. Disclosing or disseminating Trade Secret, Patent, Intellectual Property or other Proprietary Information to unauthorized parties, including news or media agencies and public forums (any social media including LinkedIn, Twitter, Facebook, FaceTime, etc.).
13. Violating copyright and intellectual property laws or the lawful rights of any individual person.
14. Falsification or misrepresentation of an Employee's identity on the Internet or in any KGiS Communications.
15. The deployment of software negligently beyond the authorised entitlement of KGiS (whether in terms of registered user numbers, geographic scope, timeframe etc.), or the installation or distribution of 'pirated' or other Software products that are not appropriately licensed for use by KGiS, or otherwise seeking to reverse engineer or hack any third-party proprietary software.
16. Usage of unauthorized peer to peer Software or external cloud Storage for file sharing from external network (Internet).
17. Exporting Software, Technical Information, Encryption Software or Technology in violation of International or Regional Export Control Laws or sanctions.
18. Moving or relocating KGiS Information Assets and Equipment without formal approval of respective Department Heads.
19. Sending or receiving files via Internet or email that may cause legal liability or harm the reputation of KGiS.
20. Sending unsolicited email messages or other advertising material.
21. Posting non-business-related messages to large numbers of users.
22. Sending, receiving, printing or accessing inappropriate, offensive or harassing statements or material.
23. Subscription to or participation in any forum, distribution service or group that delivers, distributes or disseminates illegal, inappropriate, offensive or otherwise questionable material.
24. Participating in Internet chat rooms where the subject matter is outside the scope of a job function.
25. Displaying an KGiS email address on non-KGiS websites and / or bulletin boards without authorization from KGiS Marketing Department.
26. Using KGiS resources to create a business or soliciting money for personal gain.
27. Conducting or soliciting support for political, personal, religious or charitable causes, which are outside the scope of an employee's job function and/or compliance policies.
28. Sending or forwarding chain letters, gambling, playing games or engaging in any unlawful activity.
29. Performing unauthorised actions resulting in excessive traffic on KGiS Internet and Email Systems.

30. Using an KGiS email address for personal commercial matters.
31. End users are strictly prohibited from performing any security testing, possessing or using tools for cracking software licenses, passwords and similar activities.
32. KGiS network or resource shall not be used to launch any sort of attacks/illegitimate activities within or outside INDIA. Any such action shall be dealt with serious disciplinary action followed by legal consequence.
33. Tampering or removing the equipment, software, computer, protection and security software.

8.2.5 Policy Section: Asset Tracking and Reporting

1. KGiS shall maintain the location details of Information and IT Assets along with the location history including the transfer-in and transfer-out details.
2. The location of any Information Asset shall not be changed without the approval of the designated Asset owner.
3. Physical count of the IT & other physical assets shall be carried out once in a year to ensure the validity of the Asset records.
4. KGiS shall keep an audit trail of commissioning, decommissioning or upgrade of Information Assets and log any modification and / or deletion of Information Asset records within the Asset Register.
5. KGiS ISO shall review the Information Asset Register once in a year for its comprehensiveness and ensure the register is accurate and up to date.
6. Any discrepancies found in the records resultant of the audit, physical count and reconciliation with the Asset Management Department shall be investigated and shall be reported to KGiS Executive Management.
7. Assets shall be transferred or disposed of by the designated Asset Owner with clearly communicated reasons for the transfer or disposal, transferee details, related process or task that may be affected or not due to removal of the Asset by the department and/or replacement Asset, if applicable
8. All KGiS employees and external party shall return all KGiS's assets in their possession upon termination of their employment, contract or agreements.
9. In case an employee or external party purchases KGiS's equipment or uses their own personal equipment, steps shall be followed to ensure the information is securely erased from equipment.

8.3 Policy Area: Information Classification Policy

8.3.1 Policy Section: Classification of Information Assets

1. All information stored, processed, handled and / or disseminated on Information Systems supporting KGiS as part of KGiS operational and administrative activities shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.

2. Information shall be categorized as per the below categories as well as considering the impact for each category if compromised.
    a. **Public – No Impact** – Information available in the public domain and is accessible by the general public.
    b. **Internal – Minimum Impact** – Information belonging to the company and not for the disclosure to the public or external parties.
    c. **Confidential – Internal – Medium Impact** – Information that is sensitive or confidential to the company and intended for use by identified employees who have business need to know.
    d. **Confidential** – **External –** High Impact - Information that is sensitive or confidential to the company and intended for business use only by those with the need to know (may include external stakeholders).
    e. **Sensitive – Severe Impact** – Information that is extremely sensitive or private. It is of highest value to the company and intended for use by named individuals only.
3. The current, and any previous, classification of an Information Asset shall be recorded within the Asset Register. Any changes to a classification level should be approved by KGiS ISSC with an Impact Assessment on the associated Security Control requirements being conducted.
4. Information Asset Owners shall ensure that classification levels for Information Assets under their ownership are reviewed regularly during the Information Asset's life cycle (at least annually) or in the event of a change.
5. Information Asset Owners shall be accountable for their classification.
6. Classification of an Information System or Network shall be determined by the highest classification of data resident on that Information System or transiting via that Network.

8.3.2 Policy Section: Change in Classification of Information Assets

1. Any upgrade to the classification of a specific information asset or group of information assets should be done by a change request raised via the change management system with approval from the Information Security Office and Information Owner.
2. Any downgrade to the classification of a specific information asset or group of information assets be required should be done by a change raised via the change management system to facilitate the required actions. Information owner shall seek approval from the Information Security Office along with Account/Business Function Manager with proper justification.
3. Any reclassification of asset including upgrade or downgrade of classification shall factor below parameters (but not limited to) and be assessed as applicable thereof:
    a. Change in the value of information.
    b. Change on ownership or custodianship.
    c. Changes to environment (location, access, storage, processing, usage, etc.)

d. Changes in protection levels

8.3.3 Policy Section: Labelling and Handling of Information

1. KGiS shall apply restrictions to the handling of Information of a given classification level as follows:
   a. **Sensitive:** no access to Information outside of the KGiS premises and no connection of the Information System to any transmission medium other than a secure, closed network.
   b. **Confidential- External:** no copying of data from the Information System to external media (e.g., USB). Only printing to a secure printer and printed outputs shall be shredded after use. Where authorized by the ISO or CEO, distribution or sharing of confidential documents or parts thereof to external parties will strictly be in a non-editable read only format.
   c. **Confidential- Internal:** no copying of data from the Information System to external media (e.g., USB). Only printing to a secure printer and printed outputs shall be shredded after use. Distribution or sharing of confidential documents or parts thereof to only internal employees as per business need.
   d. **Internal:** no transmission of data via public email, and printed outputs shall be shredded after use. Where authorized by the ISO or CEO, distribution or sharing of confidential documents or parts thereof to external parties will strictly be in a non-editable read only format.
   e. **Public:** no changes/alteration to the information without appropriate approval.
2. KGiS shall ensure appropriate Security Controls are in place to restrict access to Information Assets as per their classification levels from unauthorized personnel. KGiS Information Handling and Classification Procedure shall be followed for identifying, classifying and handling KGiS Information Assets.
3. All KGiS documentation templates shall support the application of classification labels via classification solution or manually with the provision of Information Classification fields in the cover sheet and header/footer of the template.
4. All KGiS documentation generated from Systems such as Enterprise Resource Planning System (ERP) shall automatically apply a watermark showing relevant classification.
5. As a default, distribution or sharing of any documentation or parts thereof produced by KGiS employees or produced for KGiS by an external party will be in a non-editable read only format, unless native format distribution or sharing is approved by the Information Security Office.

8.4 Policy Area: Information & Media Handling

8.4.1 Policy Section: End Point Security Devices

1. USB shall be restricted on all endpoints and access to removable Media shall be provided based on-line manager and ISO Approval.

2. Local admin access shall be restricted on all endpoints and access to local admin shall be provided based on-line manager and ISO Approval.
3. Only ISO approved software shall be installed on all endpoints and any additional software shall be installed based on-line manager and ISO approval.
4. All the data stored on local hard drive shall be encrypted by the approved encryption solution.
5. Vulnerability scanning shall be performed on all endpoints once in a year.
6. ISO approved minimum security baselines (MSB) should be implemented on all endpoints.
7. Any sensitive and confidential Information stored on any portable computing or storage device shall be protected, wherever applicable.
8. Laptop Users shall ensure that any KGiS related data are not stored on the local drive and instead use the KGiS One Drive as available to all users.
9. All Desktops, Laptops, Tablets, mobile phones and any other Endpoint devices provided to employees are the property of KGiS. The right to use these devices shall end either with the termination of the Employee's employment contract with KGiS or by the discretion of management, unless formally stated otherwise.
10. The Employees shall be responsible for any unwarranted damage to the devices in their possession. KGiS has the right to recover such damages from the Employees' salary based on the depreciated value of the device.
11. Any fees incurred against the personal usage of portable computing or communication devices (e.g., personal call charges in case of mobile phones where deals were brokered and supported by KGiS) shall be charged to the Employee.
12. Gaming software is not permitted for use on KGiS owned Endpoint devices, Tablets or Mobile Devices and shall not be installed.
13. KGiS devices should not be left unattended in vehicles but should a situation arise where this is unavoidable, the devices must be stored out of sight and the vehicle must be locked.
14. When devices are left unattended in the home environment they must be stored out of sight and in a safe place.
15. Laptops and other KGiS owned Endpoint devices shall not be left un-attended outside of business hours in the office environment without being secured.
16. Any files downloaded to your computer from any source (USB hard disks and memory sticks, network files, email attachments or files from the Internet) shall be first scanned for virus infections.
17. All laptops and Desktops shall be updated with the latest Operating System Patches and Service Packs.
18. Anti-virus and Anti-malware software shall be up to date with the latest signature and updates.

19. Anti-malware software shall automatically scan the external media accessed by workstation. Also, Autorun functionality to run any executable from external media shall be disabled.
20. Laptops shall be protected from environmental threats such as dust, excessive heat, and radiation with suitable measures such as using protective equipment.
21. Laptops shall be carried as hand luggage to prevent damage and unauthorized access when travelling.
22. User authentication shall be enforced for endpoint device protection.

8.4.2 Policy Section: Management of Media

1. All the external devices that contain information shall be protected against unauthorized access, misuse or corruption during transportation.
2. KGiS shall establish controls to protect media by:
    a. Using reliable transport or couriers.
    b. Contract shall be signed with the authorised courier.
    c. Maintain a list of authorized couriers that are agreed with management.
    d. Applicable procedures to verify the identification of couriers must be developed.
    e. Ensure enough packaging to protect the contents from any physical damage likely to arise during transit.
    f. Backup media movement from onsite to offsite location shall be transported using antistatic, antimagnetic and tamperproof covers.
    g. Maintain logs that identify the content of the media, record the times of transfer and relevant receipt at the destination.
    h. All back-up media shall be stored on a remote location away from the Head Office.

8.4.3 Policy Section: Disposal of Media & Documents

1. Any disposal of classified media or media containing classified information shall be approved by Information Security Office.
2. KGiS shall ensure that all electronic information and licensed software shall be properly removed when disposing of computers, hard drives and other storage devices.
3. KGiS shall ensure for the media containing confidential or higher classified Information, the data/information shall be deleted from hardware level and media shall be destroyed physically. Such destruction/disposal shall be done onsite/offsite in the presence of KGiS ISO representative. For more information on disposal, please refer to Information Classification and Handling Procedure.
4. KGiS shall ensure that media containing sensitive information shall be disposed of securely and safely, e.g., by incineration or shredding, or erasing data for use by another application within the Organization Premises.
5. Media containing non-sensitive Information shall be overwritten or formatted to sector level.

6. Corrupted and damaged media shall be evaluated for its Information content and based on the assessment; the devices shall either be destroyed or repaired after data sanitization.
7. Transferring media containing Sensitive Information within KGiS or outside shall be done using secure storage and transfer guidelines to ensure that data is protected.
8. Sensitive documents including paper documents, CD / DVD shall always be disposed using crosscut shredders.
9. When disposal of media, documents and other storage devices is outsourced, the vendor shall be evaluated based on the process followed for secure disposal methodology.
10. Disposal of media with the details of the information disposed shall be recorded to maintain an audit trail.
11. A physical document that contains any Information in relation to KGiS, its Affiliates or Clients is deemed to be classified as Confidential and can only be disposed of by means of shredding.
12. A physical document that contains any personal Information in relation to any Employee of KGiS is deemed as Confidential and can only be disposed of by means of shredding.
13. Electronic documents will be disposed of by secure deletion methods from any storage device or storage array.
    1. Electronic documents that resides on compact disks or any other single use magnetic media will be disposed of by degaussing or physical destruction of such media that renders the item unusable.
    2. Electronic documents that reside on individual computers, servers and portable storage media that are recycled or sold will be disposed of by secure deletion/sanitization or degaussing methods before these items change hands.
    3. No paper or electronic documents will be destroyed or deleted if pertinent to any on-going or anticipated government investigation or proceeding or private litigation (check with the Legal Department or the Human Resources department for any current or foreseen litigation if Employees have not been notified).
    4. No paper or electronic documents will be destroyed or deleted as required to comply with government auditing standards and regulations.

8.4.4 Policy Section: Printers and Photocopiers

1. Single dedicated printers shall only be issued to Heads and personal assistants where needed and for staff based on job requirement with Line Manager's approval.
2. Each employee's workstation shall be configured to use access controlled networked multifunction printers.
3. Printers Machines shall be securely placed so that the Confidentiality of printed Information shall not be compromised.
4. The printouts shall be labelled and handled in line with the Information Classification Policy statement defined in this document.

5. Information stored on the printers shall be configured to delete or erase automatically if the users fail to authorize the print within 24 Hours.
6. ISO approved Minimum Security Baselines (MSB) should be implemented on all shared network printers.

9 Identity and Access Management

9.1 Objective

To ensure authorized user access and to prevent and limit unauthorized access to Information and Information processing facilities.

9.2 Policy Area: Access control policy

9.2.1 Policy Section: Access and Information Classification

1. Access shall be granted to the Information in line with the classification of the Information source e.g., granting access to 'Sensitive' Information shall require authorization from respective high-level executive and scrutiny of business need.
2. Access to the Information or Information Systems shall be provided on a 'needs' basis, i.e., the access should not be more than required to discharge official responsibilities.

9.2.2 Policy Section: Unauthorized Access

1. No end user shall be allowed to gain access to any Information System through any 'User ID' not explicitly assigned to him / her.
2. Any unauthorized system access shall be reviewed, and appropriate action shall be taken if the security policy is breached.

9.3 Policy Area: Access to Networks and Services

9.3.1 Policy Section: Internet Access Control

1. Dialup access and Broadband access to the Internet are strictly prohibited while connected to KGiS Network (Wired and Wireless).
2. All software used to access the internet shall be approved by ISO and shall incorporate all appropriate / approved vendor provided security patches.
3. KGiS shall restrict and monitor the installation of any ActiveX control, flash or run Java Applet/script that may be required by any website visited by them, as these websites may be untrusted. If they wish to do so for genuine purposes, the website URL shall be provided to the ISO for verification. Upon verification and confirmation by the ISO, these controls / scripts can be installed.

9.4 Policy Area: User Access Management

9.4.1 Policy Section: User Registration and De-Registration

1. Every user shall be assigned a unique 'User ID' and no two end users shall be allowed to share the same 'User ID'.
2. User IDs of users who left KGiS shall be disabled or removed immediately (subject to handover access for ICT to extract necessary data on behalf of replacement or remaining staff).

3. Any access registration/de registration shall be governed by KGiS User Access Management Procedure.

9.4.2 Policy Section: Identity and Access Governance

1. All business applications at KGiS shall comply with basic Active Directory integration protocols such as SLDAP, and Single Sign On.
2. All business applications access shall be reviewed manually at least once in a year.
3. All application owners and business owners shall be responsible to disable/deregister native access rights on the respective applications for all the leavers of the organization.
4. Application owner and Information Security Office shall identify role-based access control for all the applications to establish basic access rights as per segregation of duties.

9.4.3 Policy Section: Provisioning of Access

1. Access to any Application, Information/System shall not be provided to anyone unless it is approved by HR, Department/ Line manager and ISO.
2. The access is essential to discharge official responsibilities for KGiS and hence is in line with the roles and responsibilities of the user.
3. The ICT shall provide basic birth right (basic access) and role specific access for all new joiners and internal movers at KGiS.
4. The employee is a current, regular, contractual or temporary employee of KGiS, or the employee is designated by KGiS having a contractual binding with KGiS for providing services that require access to the Information systems.
5. The role description is mutually agreed between both the Application/Business owner and Information Security Office.
6. The employee's request is provisioned, reviewed, and approved through KGiS's Identity Access solution by their Line Manager, Business/Application Owner and Information Security Office.
7. The employee's request is provisioned, reviewed, and approved by their Line Manager, Business/Application Owner and Information Security Office.

9.5 Policy Area: Management of Privileged access rights

9.5.1 Policy Section: Privileged Users

1. Default System accounts and vendor accounts shall be disabled on all Information Systems. KGiS Customized User IDs with administrative privilege shall be used for system level operations.
2. The privileged 'User ID' e.g., Super User ID, Default Administrative ID etc. shall not be provided to anyone (including System / Application / Database Administrators) on a permanent basis.
3. All Super-User / Administrative access shall be created with a separate User ID and default administrative User ID shall not be provided.

4. Administrative User ID shall not be used for routine activities.
5. Whenever a need arises, the default Super-User / Administrative ID shall be provided for specific tasks with the approval of ISO. After use, the password shall be changed and stored securely.
6. Information Security Office shall initiate privileged administrator users related access review for the business heads to perform access certifications.
7. All the privileged admin users that access critical systems shall be reviewed at least twice in a year by the respective line managers either by approving or revoking the credentials. Once revoked, such administrative credentials must be automatically deleted from the respective data sources.
8. All such review logs shall be maintained as identity reviews for traceability and audit logs.

9.6 Policy Area: Management of Authentication Information of Users

9.6.1 Policy Section: Authentication Methods

1. The end users shall be authenticated by various techniques like Passwords, Smart Cards, Smart Tokens, Biometrics Devices, etc. depending on the criticality of the Information resources to be accessed.
2. The computers accessing KGiS Information resources shall be authenticated by various methods like MAC address.
3. Scripts or utilities shall be used to authenticate the validity of Applications accessing the Databases or other Applications.

9.7 Policy Area: Review of User Access Rights

9.7.1 Policy Section: Automated User Access Reviews

1. Review of all employee's logical access rights shall be initiated by Information Security office to be verified and validated by respective line manager once a year.
2. Privilege identities (System and Functional administrators including generic accounts) shall be reviewed at least once every 6 months by line manager and signed-off by information security office.
3. Business owner access review for critical applications shall be conducted once in a year or on ad-hoc basis.
4. Data Centre physical access review to the main hall shall be reviewed once every quarter by the line managers and signed-off by ICT operations with monitoring by information security office.
5. Third-party users (external parties) accounts shall be reviewed and validated every 6 months by information security office in coordination with the requester for extension or removal of access rights.

6. All the sensitive information such as account details and password of all KGiS employees shall be encrypted.

9.8 Policy Area: Removal or adjustment of access rights

9.8.1 Policy Section: Access Revocation

1. The access to the Systems shall be revoked as soon as it is not required to discharge the official duties for KGiS.
2. The access to the system shall be revoked in a manner so that it is possible to track the history of activities performed by the end User.
3. End users shall be disabled from all Systems as soon as their services are terminated from KGiS as a result of resignation, termination, retirement, contract termination, etc.
4. In case of transfer of the end users to other departments / functions, their 'User ID' shall immediately be disabled from all Information Systems that are not required for discharging the new responsibilities.
5. In case of transfer of the end users to other departments / functions, old user profile access from all Information Systems shall be immediately revoked and new user profile with new designation and access based on the role assigned shall be granted after approved from line manager and Information Security Office.
6. It is the responsibility of HR Department and the relevant business department to inform the ICT at least one day before the required date of access revocation.

9.9 Policy Area: System and Application access control

9.9.1 Policy Section: Information access restriction

1. The information and communication system privileges of all users, systems and independently operating programs such as agents, shall be restricted based on the need to know. This means that privileges should not be extended unless a legitimate business-oriented need for such privileges exists.
2. The information owners and ICT shall only grant the minimum level of access required for users to successfully complete their job functions.

9.9.2 Policy Section: Secure log-on procedures

All access to systems and applications shall be controlled by a secure log-on procedure.

9.10 Policy Area: Password Management System and Criteria

9.10.1 Policy Section: Usage of Passwords

All Workstations, Servers, Applications, Infrastructure devices, Database, Operating System, and Critical Electronic Documents shall be protected with strong and effective passwords.

9.10.2 Policy Section: Password Standards

1. The passwords shall contain at least 8 alphanumeric characters.
2. The password shall be case sensitive and shall contain the combination of upper and lower case (e.g., a-z, A-Z).
3. The password shall have at least one special character e.g., 0-9,!@#$%^&*()_+|~- .
4. A "User ID" shall not be used as a password (either as it is, reversed or in upper case).
5. The password shall not be a word found in dictionary or a country name or a company name.
6. The passwords shall not be personal information such as first, middle or family name, birth date, initials, names of family members etc.
7. Maximum password age shall be configured to be 90 days.
8. Minimum password age shall be configured to be 1 day.

9.10.3 Policy Section: Password Maintenance

1. All System-level passwords (e.g., root, enable, operating system admin, application administration accounts, etc.) shall be changed after every 90 days.
2. All User-level passwords (e.g., email, web, desktop computer, etc.) shall be changed every 90 days.
3. Password history shall be enforced for five iterations i.e., during password change users shall not be allowed to reuse the last five passwords.
4. Account lockout to be implemented on KGiS systems as per below requirements:
   a. Workstations - 5 failed/invalid logon attempts
   b. Servers - 10 failed/invalid logon attempts
5. In case of any legacy systems or systems that do not support above requirement, the account lockout can be implemented for fewer invalid logon attempt(s), but not 0. This must be explicitly approved by ISO.

9.10.4 Policy Section: Password Protection

1. Password shall be protected by the Users and Users shall be responsible for the activities performed through their 'User ID'.
2. Passwords shall not be shared with anyone including Family, Co-workers or support teams (e.g., WPO/Field & Workplace Support).
3. Users shall not write passwords down and store them anywhere.
4. Passwords shall not be stored in a file on any computer system without encryption.
5. Users shall take care not to type the passwords while being observed.
6. Passwords shall be masked / obscured on the display while Users type it.

7. Passwords shall be communicated to users via secure methods and refrain sending credentials using same communication medium.
8. The 'Remember Password' feature of applications / systems shall not be used.
9. If employees suspect that their password has been compromised, they shall immediately change their password and notify the incident to the ICT Service Desk.
10. All passwords shall be classified as 'Confidential'.
11. Users should be very cautious while entering passwords and shall ensure that passwords are entered only in correct password filed provided.
12. Users shall exercise extreme care and due diligence while using passwords in presence of others or in public places etc.

9.10.5 Policy Section: Privileged User Passwords

1. All default passwords of highest privileged accounts like Super User, Root and Administrator shall be changed as soon as the system becomes operative.
2. The Privileged User passwords shall follow the above-mentioned standards and shall:
    a. Have a length of at least 14 alphanumeric characters.
    b. Not be granted to anyone on a permanent basis.
3. The log of issuance of the Privileged User passwords shall be maintained and reviewed along with the purpose of issuance.

9.10.6 Policy Section: Use of privileged utility programs

1. A privileged account may or may not be associated with an individual. If the account is not associated with an individual, it should provide an audit trail pointing back to an authorizing user. These accounts should be kept to a minimum, individually approved, documented and strictly limited to those with a business justification for use.
2. The authority and access to use advanced operating system utilities and commands that bypass system access controls should be monitored, logged, reviewed and restricted to those individuals who require access to perform their job functions.

9.10.7 Policy Section: Access controls to program source code

1. Audit log of all access to program source libraries shall be maintained.
2. Source control software shall be used.
3. Program source libraries shall exist for development, test and production.

10 Cryptography

10.1 Objective

To ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.2 Policy Area: Use of Cryptography Controls

1. KGiS shall develop and implement the use of cryptographic controls for protection of Information classified as "Confidential" and above.
2. KGiS Key Management Procedure shall govern the use, protection, and lifetime of cryptographic keys through their whole lifecycle (i.e., issuing, changing, and revoking of keys).
3. KGiS shall select cryptographic key length that shall provide adequate protection as per the Information Security Design, key length recommended below is for Information of classification "Confidential" and above, as follows:
    a. For symmetric/secret key cryptography, key lengths of at least 256 bits shall be used; and
    b. For asymmetric/public key cryptography, key lengths of at least 2048 bits shall be used. (For legacy systems, where 2048-bit encryption cannot be implemented, approval to be obtained from ISO)
4. Only Infosec approved cryptographic controls shall be used.
5. The usage of cryptographic controls shall comply with the latest cryptography standards such as AES, DES (Data Encryption Standard), Blowfish, RSA, IDEA, Diffie-Hellman, etc.
6. KGiS shall ensure advanced encryption mechanism shall be deployed (e.g., Digital Signature) while exchanging critical and sensitive government contracts and information.
7. The ISO shall be consulted during defining the type and quality of encryption algorithm that shall be used and length of cryptographic keys, as per the value and classification of information along with the tools and applications to be used for data encryption.

10.3 Policy Area: Key Management

KGiS shall select cryptographic key length that shall provide adequate protection as per the Information Security Design, key length recommended below is for Information of classification "Confidential" and above, as follows:

1. For symmetric/secret key cryptography, key lengths of at least 256 bits shall be used; and
2. For asymmetric/public key cryptography, key lengths of at least 2048 bits shall be used. (For legacy systems, where 2048-bit encryption cannot be implemented, approval to be obtained from ISO)

3. Encryption keys shall be generated automatically, so that no user shall have the opportunity to expose a key or influence key creation.
4. Encryption keys are the most sensitive type of information, and access to such keys shall be strictly limited to those who have a need-to-know.
5. Procedures to revoke/block keys and to repair damaged or corrupted keys shall be defined.
6. All cryptographic keys shall be protected from modifications and loss.

10.4 Policy Area: Use of Encryption

1. All laptops local hard drives shall have encryption enabled prior to their use.
2. Information classified as Sensitive or Confidential, which is stored in removable storage devices, shall be encrypted.
3. Information classified as Sensitive or Confidential, transmitted through email to another domain shall be encrypted. The key for decrypting the information shall be communicated through alternate channel to avoid compromise of information.
4. All remote access to information systems shall be provided through SSL enabled VPN connections along with Multifactor Authentication (MFA).
5. All information, classified as Sensitive or Confidential, transmitted through wireless networks shall be encrypted using WPA2 (Wi-Fi Protected Access) in minimum.
6. Users shall not install any third-party encryption software that is not approved by Information Security Office.

11 Physical and Environmental Security

11.1 Objective

To prevent unauthorized physical access, damage, and interference to KGiS Information and Information processing facilities.

11.2 Policy Area: Secure Areas

11.2.1 Policy Section: Physical and Security Perimeter

1. The areas in the physical boundary of KGiS Offices shall be classified in terms of their Physical Security requirements and the classifications shall be documented.
2. All secure areas shall be assigned with the owner for assigning/re assigning the classification and ensuring the implementation of security measure, as appropriate.
3. Risk Assessment shall be performed annually, and respective Security requirements shall be developed and documented for critical areas.
4. The selection and design of a secure area shall take into account the possibility of Security lapses due to unauthorised access.
5. KGiS shall ensure that the external walls, doors and windows are properly strengthened, secured and monitored to prevent unauthorised and / or covert access.
6. Suitable Intruder Detection Systems (IDS), including video surveillance cameras, shall be installed as perimeter defences and shall be tested for proper functioning on a regular basis.

11.2.2 Policy Section: Physical Entry Controls

1. Access to Information processing facilities shall be restricted to authorized personnel based on job roles and pre-arranged site visits / inspections.
2. Access rights to secure areas shall be reviewed on a Half-yearly basis.
3. Access to all critical areas shall be monitored and logs or audit trails shall be maintained and reviewed on a periodic basis.
4. Appropriate authentication controls, e.g., passwords, PIN, swipe cards, biometric devices etc. shall be implemented to validate all authorized physical access.
5. All personnel shall be required to wear visible identification and are encouraged to challenge unescorted strangers and anyone not wearing visible identification.

11.2.3 Policy Section: Securing offices, rooms and facilities.

1. All visitors (vendors, partners, ex-employees, interview candidates) to KGiS's office building shall be escorted by respective employee's right from the reception till the departure.
2. KGiS's security guards shall ensure that there is no tail gating by any visitor or an employee.
3. KGiS's security guards shall only allow visitors to the office facility only if an access card is issued and the presence of a valid ID card is visible with an KGiS's employee accompanying them.

4. KGiS's visitor's reception shall validate the presence of an KGiS's employee to receive before the issuance of an access card to the designated floor in the facility.
5. Visitors including Third Party organization personnel shall be granted supervised access to Information processing facilities for maintenance tasks or other specific and authorized purposes only.
6. Visitors and Third-Party organization personnel shall be instructed on the security and emergency requirements and procedures of the specific area visited.
7. A visitor's register shall be maintained with purpose, date and time of entry and departure shall be recorded and reviewed on a regular basis.
8. All Data Center visitors (Vendors, Partners) shall always be escorted by KGiS business personnel and security guards for access to restricted areas.

11.2.4 Policy Section: Visitors and Third-party access

1. Visitors and Third-Party organization personnel shall be granted supervised access to Information processing facilities for maintenance tasks or other specific and authorized purposes only.
2. Visitors and Third-Party organization personnel shall be instructed on the security and emergency requirements and procedures of the specific area visited.
3. The date and time of entry and departure of Visitors and Third-Party organization personnel shall be recorded and reviewed on a quarterly basis.
4. Data Center visitors shall always be escorted by KGiS personnel or security guard for access to restricted area.

11.2.5 Policy Section: Protecting against external and environmental threats

1. Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
2. External authorities and specialist's advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

11.2.6 Policy Section: Working in secure areas

1. Employees should only be made aware of activities within a secured area on a need-to-know basis.
2. Sensitive materials should be locked in secure cabinets immediately after use.
3. All desks and screens should be cleared, and workstations locked immediately after use.
4. Networked computers should be password protected and have active screen savers.
5. Workstation activity should be monitored to identify unauthorized access.
6. Unsupervised personnel working in secure areas should be avoided to prevent malicious activities.

7. Third party support services employees should be granted restricted access to secure areas only when absolutely required.
8. Third party access should be authorized and monitored.
9. Photographic, video, audio or other recording equipment should not be allowed.

11.2.7 Policy Section: Delivery and loading areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. The entity shall:

1. Establish access procedures to loading and unloading areas to restrict access to only authorized personnel.
2. Physically segregate loading and unloading activities.
3. Inspect and register incoming and outgoing material in accordance with the entity's asset management procedures.

11.3 Policy Area: Equipment Security

11.3.1 Policy Section: Equipment sitting and protection

1. Air conditioning and humidity controls shall be installed in the computer room/datacentre and these controls should operate continuously and be available twenty-four (24) hours a day. The following controls to be implemented:
2. Air conditioning equipment should incorporate machine redundancy such that the failure of any one component will not interrupt the air conditioning of the computer room:
    a. Climate control equipment should be properly labelled.
    b. Climate control equipment that is stacked on racks should have proper ventilation.
    c. Climate control systems should be supported by a generator with an operating time of at least sixty (60) minutes to ensure proper close down of system impacted.
3. Temperature at server inlets and humidity levels by dew point should be measured.
4. All computing facilities and all occupied areas should be provided with automatic fire suppression equipment as required by local fire regulations for electrical equipment.
5. Computer environments, including temperature, humidity and power supply quality should be monitored to identify conditions which might adversely affect the operation of computer equipment, and to enable immediate corrective action to be taken.
6. Critical computing environments shall be monitored for water or moisture conditions, which could adversely affect the operation of information resources. These water and moisture monitoring devices shall be installed in all critical information processing environments, including facilities that are either remote or unoccupied.

11.3.2 Policy Section: Supporting Utilities

1. The entity shall protect equipment from disruptions caused by failures in supporting utilities. Supporting utilities shall:
    a. Be tested for any malfunctioning.
    b. Ensure protection and uninterrupted power supply on information systems.
    c. Provide emergency lighting in case of main power failure.
    d. Have up-to-date utilities maintenance logs.

11.3.3 Policy Section: Cabling security

Cabling and line facilities supporting voice and data communications should be protected with controls consistent with corporate requirements for physical and environmental controls such as alternative power supplies, physical access and environmental management facilities.

11.3.4 Policy Section: Equipment maintenance

1. Preventive maintenance shall be performed regularly on all equipment used to support information systems or data center operations in conformance with manufacturer recommendations. This includes hardware for IT platforms (servers, disk arrays, cabling, etc.) and data center environmental and security equipment (fire suppression, environmental controls, etc.) All maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel should be inspected for obvious improper modifications.
2. Organization shall train the personnel to verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices, create awareness to report any suspicious behaviour and indications of device tampering or substitution to appropriate personnel.
3. Maintenance personnel who do not possess necessary access authorizations, clearances, or formal access approvals shall not be allowed to secure areas.
4. Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
5. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.
6. Predictive maintenance activity shall be scheduled when it is most cost-effective and before the equipment loses performance within a defined threshold.

11.3.5 Policy Section: Removal of assets

1. Any equipment shall not leave the facility of the organization without permission (this is also applicable to the information and the software)
2. KGiS shall establish control of equipment that leaves the company's facilities by defining, e.g., what is the reason, who is in charge of the equipment, how much time it will be out, where it will be etc.
3. All equipment that is removed should be logged out and logged back when returned.

11.3.6 Policy Section: Security of equipment and assets off-premises

1. Equipment, including personal computing devices and portable or handheld devices must be physically protected from security threats, environmental hazards, and maintained according to manufacturer's specifications.
2. The environmental security equipment's such as Air Conditioners, Humidity control equipment's, fire suppression systems, smoke detectors, temperature and humidity monitoring devices etc. shall undergo regular maintenance as per the manufacturer's recommendations and records will be kept
3. The environmental security equipment's shall undergo regular tests (once a year at least) and test results shall determine the efficiency and adequacy of such equipment's
4. Hazardous and combustible materials shall be stored at a safe distance from data center, server rooms and equipment rooms
5. Adequate security controls shall be implemented on the equipment and information, which are located or hosted outside the organization premises (off-site facilities), to reduce the risk of unauthorized access to data and to protect against loss or damage.
6. Any equipment or media taken off-premises must not be left unattended in public areas. Lost or stolen computing devices must be reported immediately to the business unit management and Information Security Department.
7. Electric and telecommunications cabling should also be segregated to avoid interference.

11.3.7 Policy Section: Secure disposal or re-use of equipment

1. Secure disposal procedures shall be proportional to the information classification level: The higher the classification, the greater assurance that information cannot be retrieved after disposal. Best disposal practice like Shredding or incineration of the media shall be followed.
2. There shall be clear identification of Information that requires secure disposal with the usage of watermarks, or coloured border to identity the type of information for secure disposal.
3. KGiS should avoid disposing large quantities of accumulated media instead plan for defining short accumulation period or small storage volume to execute the disposal procedures.
4. KGiS shall ensure that all the items were properly disposed with proper listing of log information, who performed the procedure, when and what was the method used thereby keeping traceability of sensitive disposed items.
5. Verify the equipment prior to disposal to ensure there is no media contained in the equipment by using a disposal checklist.
6. For highly sensitive information based on the information classification, KGiS shall advocate the use of non-retrievable methods such as physical destruction (grinding, shredding) or overwriting as disposal techniques.
7. Disposal of KGiS assets/equipment carrying sensitive information shall be performed onsite or offsite in presence of KGiS ISO representatives.

8. Any device that requires to be sent for damage assessment, warranty or replacement, Information security shall evaluate the equipment for encryption, device protection and data privacy and determine whether the device should be physically disposed instead of sending to any other offsite location.

11.3.8 Policy Section: Unattended user equipment

1. KGiS shall deploy adequate physical protection measures on Information processing facilities (i.e., data centers, computer rooms, sensitive or privacy related data such as financial transaction data, payment and credit card data, healthcare data, etc.)
2. KGiS shall employ an annual penetration testing process that includes unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.
3. All important papers and removable storage media such as CDs and diskettes against theft or copying, shall comply with a "clear desk" policy, providing lock-out on unattended terminals, and restricting physical access to important post/fax points.

11.3.9 Policy Section: Clear desk and clear screen policy

1. All desks shall be kept clean, tidy, and clear of sensitive or valuable KGiS assets while left unattended and at the end of each working day, all assets shall be secured.
2. Work desks and work areas shall be kept as clear as possible at all times; in particular customer records or other identifiable personal or business Information shall not be held on the desk within reach / sight of Visitors.
3. Laptops and other portable and mobile devices shall be secured or removed from open area workstations at the end of each working day.
4. Lockable credenzas, storage/filing cabinets or cupboards shall be provided to all Employees to lock away any documentation and other Information media at the end of the workday.
5. Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office / room doors shall be locked if left unattended.
6. In the meeting rooms, at the end of each session all Sensitive Information shall be cleared including flipchart sheets and whiteboards.
7. The Windows Screen Lock shall be enabled (via Active Directory Group Policy) when there is no activity on a workstation for more than 15 minutes. The same shall be password protected for reactivation.
8. When left unattended, Laptops and Workstations shall be secured by one of the following methods:
    a. A password-protected screensaver with the automatic activation feature set at 15 minutes or less. The screensaver shall not be deactivated without prior permission; and
    b. By locking the System (press Ctrl-Alt-Delete and then select the "Lock Computer" option or “Log-off” option).

12 Operations Security

12.1 Objective

To ensure effective management of Information security controls are incorporated in IT Operational activities.

12.2 Policy Area: Operational procedures and responsibilities

12.2.1 Policy Section: Documented Operating Procedures

1. Operating procedures shall be developed by respective process/application/system owners for each critical information system or application that forms part of the Information processing facilities including the tasks and responsibilities of personnel involved.
2. Operating procedures shall be developed to allow for the correct, consistent, and secure development, introduction, management and retirement of information assets.
3. Baseline configuration documents for different technologies in relevance to information security and compliance shall be documented, maintained and followed for any existing and new information systems within KGiS organization.
4. Operating procedures shall be maintained and updated when necessary or if a change or an upgrade occurs.
5. Operating procedures shall be reviewed periodically to ensure continued relevance and accuracy to the work being undertaken.
6. KGiS shall follow quality management system guidelines to authorize changes to operating procedures.
7. Responsibilities for development of appropriate operating procedures within each service team shall be defined.
8. Documented operating procedures shall specify the instructions for the detailed execution of each job, at a minimum, including:
    a. The installation and configuration of systems;
    b. Proper processing and handling of Information (including backups) both automated and manual;
    c. Scheduling requirements, including interdependencies with other Systems, earliest job start and latest job completion times;
    d. Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
    e. Support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;

f. Special output and media 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;

g. System restart and recovery procedures for use in the event of System failure;

h. The management of audit trail and System log Information; and

i. Monitoring procedures.

9. Operating procedures and the documented procedures for system activities shall be treated as formal documents and changes to the same shall be authorized by the owner. Where technically feasible, Information systems shall be managed consistently, using the same procedures, tools and utilities.

12.3 Policy Area: Change Management

1. All changes to the live or production data processing systems or environment, critical or non-critical shall follow KGiS change management process.
2. All changes to any other systems or facilities that might have an impact on the confidentiality, integrity and / or availability of information assets shall follow KGiS's change management process and all significant changes are risk assessed and approved in the CAB meeting on a weekly basis.
3. All major and significant changes shall be assessed for risk and tested before being implemented on production Information Systems.
4. When changes are made, an audit log containing all relevant Information to the change shall be retained.
5. Incident ticket number shall be updated in the change tickets to keep track of incidents resulting the change.

12.4 Policy Area: Capacity Management

1. Capacity Plan shall be developed and maintained by the ICT Team in line with KGiS business requirements as outlined in the collective KGiS Service Level Agreements (SLAs).
2. The capacity plan shall compare current and predicted performance and availability requirements with present and planned capacity of IT infrastructure and resources.
3. IT resource performance and capacity shall be monitored, analysed on a yearly basis to minimize the risk of service disruptions due to insufficient capacity or performance degradation.
4. The IT capacity plan shall describe measures taken and planned for maintenance and enhancement of IT capacity.
5. The operational capacity requirements of new systems should be identified, documented and tested prior to their acceptance and use.

6. Methods, procedures, tools and techniques shall be identified to monitor capacity, tune performance and provide adequate capability.
7. Time scales and utilization and / or performance thresholds for all critical IT components shall be identified and monitored.
8. The capacity of the IT infrastructure resources shall be monitored according to the requirements in terms of various performance indicators like Response Time objective, storage capacity and Fault Tolerance.
9. Excess capacity shall be identified for possible redeployment.
10. An exception report shall be produced and maintained by the ICT team on a monthly basis along with the recommendations for corrective actions.

12.5 Policy Area: Separation of Development, Test and Production Environments

1. Development, test and production environments shall be separated logically and / or physically to reduce operational risk of unauthorized changes.
2. Rules for the transfer of software from development to operational environmental shall be defined and documented.
3. Compilers, editors, and other development tools or system utilities shall not be accessible from operational systems when not required.
4. Users shall use different login profiles for operational and test systems, and menus shall display appropriate identification messages to reduce the risk of error.
5. Sensitive & Confidential data shall not be copied into the test environment. If need arise, then the information shall be encrypted or masked or scrambled before being used in the test environment.
6. Developers shall not introduce untested or malicious code on production systems.
7. The migration of code to the operating environment shall happen with planned beta testing using test environments.
8. Access to development, test, and operational environments shall be managed by privilege identity management solution of KGiS.
9. Test data should be masked, scrambled and encrypted when used in the testing or development environment based on data classification and criticality. Any exception to these shall be exclusively approved by ISO.

12.6 Policy Area: Protection from Malware

12.6.1 Policy Section: Control against Malware

1. KGiS shall employ, configure, and manage corporate anti-malware and end-point detection and response (EDR) mechanisms for the network as well as all domain and workgroup workstations, laptops, servers of KGiS and any other devices connected to its network.

2. KGiS shall ensure that anti-malware & EDR software is up-to-date and operates on a real time basis on all KGiS servers and workstations.
3. KGiS shall ensure that the end users shall not be allowed to install, uninstall or change the configuration settings of the anti-malware, EDR software or any other security solution installed for the sanctity of the system.
4. Anti-malware software shall be configured to do a full system scan at least once a week and a real time scan of all the files from removable media when they are accessed, copied or moved.
5. Anti-malware management server is configured and in sync with the active directory server.
6. KGiS shall configure servers, workstations and laptops, so that they do not "auto-run" contents from removable media.
7. Anti-malware and EDR software shall be configured to quarantine the infected files if they cannot be cleaned.
8. Security administrator shall ensure the anti-malware server configurations are hardened as per approved KGiS minimum security baseline (MSB) document.
9. New anti-malware software signatures, virus pattern files and scan engine shall be applied within 24 hours of its release by the vendor.
10. All KGiS endpoint devices shall be configured to allow automatic updates.
11. Anti-malware software on e-mail servers shall be configured to scan all internal and external mails including all email attachments before it reaches an end user's mailbox.
12. Anti-malware software on the Internet gateways shall be configured to scan all incoming / outgoing Internet traffic.
13. Exclusion list needs to be developed in line with business requirements and the same list needs to be approved by ISO.
14. Anti-malware software checking shall be enforced as part of the boot sequence on all workstations, laptops, and servers of KGiS.
15. KGiS shall ensure the personal systems of third-party vendors and consultants including remote users are updated with reliable antivirus application. If not, access to KGiS network resources shall not be granted.
16. Anti-malware client shall be enabled automatically as and when the desktops, laptops, and servers are started / restarted.
17. Anti-malware software shall be configured along with Web security to scan all webpages (URLs) for any malware infected website.
18. Anti-malware servers shall be integrated with SIEM solution to analyze and alert any security incidents.
19. Logging shall be enabled and access to antimalware system settings and Antimalware log files shall be restricted.

20. Antivirus logs shall be stored online for 90 days and will be reviewed by security operations team.
21. Redundancy shall be built for Anti-malware software server.
22. Recovery test for anti-malware software servers shall be conducted periodically.
23. KGiS shall ensure that all end users are aware of malware risks, behaviours and preventive actions.
24. All end users shall report any malicious content detected on their systems and endpoint devices to KGiS Service Desk.

12.7 Policy Area: Backup

12.7.1 Policy Section: Identification and Planning

1. All Information, application, systems and network and security devices shall be identified and documented along with the required back-up parameters.
2. All Information, desktop, application, systems and network and security assets shall be configured for backup as per defined required back-up parameters.
3. All KGiS information/data accessed from workstations, laptops, or other portable devices should be as per backup cycle and policy.
4. Information backup parameters (i.e., schedule, back-up type, etc.) shall be identified and approved by business and service owners.
5. At a minimum three versions of system state backups shall be maintained.
6. Backup schedule shall be maintained via automated applications or performed manually.
7. All assets are required to be qualified for backup prior further processing.
8. The frequency of backups is determined by the RPO value of systems and the retention period for backup copies is determined by the criticality of the data.
9. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) shall be considered for business-critical data to comply with business continuity management.

12.7.2 Policy Section: Backup and Monitoring

1. All Information systems, network and security devices shall be backed up as per agreed schedules with business and system owners.
2. The frequency and extent of backups must be in accordance with the recovery time and recovery point objectives and the acceptable risk as determined by the Business Impact Analysis and the data owner.
3. Data backups shall be recorded on physically separated storage Media (e.g., another machine, Optical or Tape Media, Removable Disks, etc.).
4. KGiS shall ensure that the storage media has adequate storage capacity for the quantity of data to be stored for each backup based on capacity analysis result.

5. The backup data shall be recorded on a medium and in a format where readability can be assured to restore the data on existing as well as planned technologies.
6. The storage media and its supporting hardware and software shall be based on proven technology and open standards.
7. The storage media used shall have a low susceptibility to physical damage and be tolerant of a wide range of environmental conditions without data loss.
8. The reuse of storage media shall be planned carefully to avoid any possible data or backup cycle loss due to media overwrites.
9. Any configuration change to the information systems shall be backed up and DR backup list for restoration shall be updated for proper business continuity.
10. The electronic data backup and recovery process for each system must be documented and periodically reviewed.
11. Physical access controls shall be implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest sensitivity level of information stored and in accordance with information classification policy requirements.
12. Facilities and procedures between KGiS and the offsite backup storage vendor(s) shall be audited periodically.
13. Backup tapes must have an identification bar code mapped to media information database in the backup solution.
14. Whenever connected to the corporate network, any information stored on a local drive on employee endpoint devices are backed up through automated backup & recovery solution.
15. Instead of storing official data on corporate laptops or workstations, all employees shall use the allocated shared **department folders** in a readable format to ensure it is backed up daily. **OneDrive** can also be used for short term storage/backup or an alternative to email for sharing the document.

12.7.3 Policy Section: Backup Configuration and Log files

1. Backup of anti-malware software servers, configuration and log files shall be taken on a monthly basis or before any change execution and stored off-site.
2. Backup of firewall and critical network components configurations shall be taken on a monthly basis and stored off-site.

12.7.4 Policy Section: Backup Testing and Restoration

1. Backup arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans.
2. Backed up data from critical application shall be restored at least once a year to ensure that it is recoverable, and a recovery test log shall be kept.
3. Approval from the business and service owners shall be required prior testing or restoration of the assets.

4. Restoration procedures shall be checked and tested on an annual basis to ensure that they are effective and can be completed within the time allotted in the operational procedures for recovery.
5. The restoration results shall be shared with the ISO in order to validate with recovery point objective from business continuity management system.

12.7.5 Policy Section: Backup Media Retention

1. Backups of all KGiS's Information system records and software must be retained such that computer operating systems and applications are completely recoverable. This may be achieved by using a combination of techniques such as system state, image copies, incremental backups, differential backups, transaction logs, or other techniques.
2. The backup media used shall have a life span in accordance with the retention requirements of data and comply with KGiS's data classification policy and framework
3. At a minimum, backup copies of data shall be retained for a **period of 7 years.**
4. At a minimum, one fully recoverable version of all KGiS Information systems records shall be stored in a secure, off-site location. An off-site location can be at an off-site vendor storage facility.
5. Backup tapes shall be encrypted / password protected before they are stored onsite or at offsite facility.
6. **Permanent Retention:** Unless otherwise specified all documents pertaining to the list below will be kept for an indefinite period:
    a. Shareholder and Board resolutions;
    b. Board minutes;
    c. Articles of Association; and
    d. Annual Reports.
7. **General Retention:** Unless otherwise specified all documents pertaining to the list below will be retained for a minimum period of **7 (Seven) years:**
    a. General Asset Information;
    b. Human Resources;
    c. Company Financial Records;
    d. Contracts (After Expiration); and
    e. Client Documentation, reports and deliverables

12.7.6 Policy Section: Backup Media Maintenance

1. Arrangements shall be made to ensure that backup media is protected against physical threats e.g., misplacement, theft, fire, humidity, dust, etc.

2. Access to the backup media shall be restricted and a procedure shall be implemented to ensure authorized access to backup media for restoration or disposal.
3. Procedures shall be implemented to ensure that backup data are quickly identifiable and accessible when required.
4. In case of movement of the backup storage media, proper handling and taking-over procedures shall be implemented.
5. A copy of the data backup shall be stored off-site to ensure data protection and availability in case of a disaster.
6. KGiS shall inspect/audit the third-party off-site storage facility on an annual basis to ensure compliance with agreed security measures.

12.7.7 Policy Section: Backup Media Disposal

1. Damaged, aged, dysfunctional or redundant backup media shall be disposed of only after the approval of the ISO.
2. KGiS shall ensure that the data on the backup media is not accessible / readable by any means after disposal.
3. KGiS shall ensure that the backup media is disposed of in most environmentally friendly manner.
4. KGiS shall validate the data classification parameters while disposing backup media and choose secure disposal mechanisms per criticality of data.
5. All media disposal shall follow secure disposal policy (media/document/equipment) requirements stated earlier in this document.

12.8 Policy Section: Logging and Monitoring

12.8.1 Policy Section: Logging

1. All appropriate end user management activities shall be logged and reviewed.
2. The information access like user login, logout, login failure, password change, etc. shall be logged and reviewed.
3. The activities performed through privileged 'User ID' shall be logged and monitored.
4. Logging shall be enabled on all the critical devices including application servers, network devices and security devices.
5. The application's error / exception handling capability shall log all error and failure events to an error / failure log.
6. Logging requirements shall be determined based on scope, Information to be captured in security logs, frequency for review of security log data, and applicable laws and regulations.
7. The critical log sources shall be configured for log generation.
8. Logs generated for activities that affect the availability and security of the systems, shall be configured for monitoring.

9. All denied attempts to any port, protocol, or service shall be logged and multiple attempts shall be reported to ISO.
10. KGiS shall ensure that administrator logins, changes to the administrator group, Administrator addition and account lockouts are logged and monitored.

12.8.2 Policy Section: Logging Parameters

1. Logs shall capture the below details at minimum:
    a. User IDs
    b. Date and Time
    c. Details of the event
    d. Terminal identity or location where possible
2. Following log types shall be monitored:
    a. Security Logging
    b. Administrative and Operator Logs
    c. Fault Logging
    d. Backup logs

12.8.3 Policy Section: Protection of Log Management

1. Centralized log server shall be deployed for collecting; storing and analyzing the logs generated by the servers, network and security devices.
2. The Security Operations Centre team (SOC) shall analyze the logs for all activities that affect the security of the system.
3. A separation of roles shall be considered between the personnel undertaking the review and those monitoring the logs.
4. Unauthorized activities identified during the log reviews shall be reported to the ISO.
5. All security logs shall be maintained at least for 6 months (onsite) and 6 Months (offsite) and no one shall be allowed to disable, modify, or delete the logs without formal permission from the ISO.
6. The log of issuance of the privileged end user passwords shall be maintained and reviewed along with the purpose of issuance. The audit Log shall bind the individual ID of the end User causing (or associated with) the audited event to the audit record for that event.
7. The audit facility used by the application shall ensure that the application's audit records are protected from deletion or unauthorized modification.
8. It shall be ensured that the DHCP server is configured to log hostnames or MAC addresses for all clients and all logs are stored online for 6 months and offline for 6 months.
9. Logs for security devices such as Firewalls, IPS's, IDS's and Web filters shall be configured and reviewed through SIEM.

10. The audit log data shall be backed up and shall be protected from deletion.
11. The audit trail events shall be stamped with accurate date and time and shall include source IP, destination IP, protocol used, and action taken.
12. Adequate security controls shall be taken into account while transferring the logs from the source to the centralized log storage to protect confidentiality, integrity and availability of the logs.
13. Access to the logs shall be strictly controlled. No user shall be granted permission to modify the logs in an unauthorized manner.
14. System owners/administrators shall not be granted access to the log repository.
15. Log repository shall be hardened as per the applicable security baseline documents.

12.8.4 Policy Section: Administrator and Operator Logs

1. ICT Administrator activities shall be logged across all the servers, devices, etc. and administrator logs shall be reviewed periodically through SIEM.
2. ICT Administrator logs shall never be deleted and due to lack of system space, shall be archived and stored at the approved off-site storage facility.

12.8.5 Policy Section: Log Monitoring, Analysis & Review

1. Logs generated and stored shall be monitored in real time by a central log monitoring system.
2. The central log monitoring system shall be capable of centralization, sorting and parsing of the logs collected from different IT Systems to identify, contain and respond quickly to events/incidents in the network.
3. Security monitoring team shall centrally monitor the logs generated by all the IT systems.
4. Logs shall not be analyzed by the same individual whose activities are being logged and monitored, to ensure segregation of duties.
5. Corrective and preventive measures on reported incidents shall be taken.
6. Logs shall be backed up on a regular basis as per the Backup policy.
7. On monthly basis the Security monitoring team shall submit log analysis reports to the ISO including trends on critical system or security events.
8. Security monitoring systems shall be kept current and regularly tested to ensure that desired events are detected, and the system performance is efficient, accurate and current.
9. The action that needs to be taken for critical alerts shall be identified and documented by the Security Monitoring team in accordance with the Security Incident Management Procedure.

12.8.6 Policy Section: Time Synchronization

1. All system clocks shall be synchronized to ensure the accuracy of audit logs.
2. The date/time format and standard time to be used in all systems shall be defined.

12.9 Policy Area: Control of Operational Software

12.9.1 Policy Section: Installation of Operational Software

1. KGiS shall ensure that only licensed copies of software and/or applications are installed on any of the KGiS owned computing systems or standalone computing assets.
2. A software library shall be created from KGiS approved software list and maintained.
3. Software from the KGiS approved software list shall be installed on KGiS Information systems.
4. Information Security Office shall monitor the installation of software packages and applications to ensure that software-licensing agreements are strictly adhered to.
5. Critical software shall be tested in a test instance prior to introduction in production environment to ensure compatibility with the business applications.
6. For all software installation, approval from system owner and Information security office shall be formally obtained.
7. KGiS shall ensure that modifications even minor changes to software / applications, be installed into a live environment after obtaining the approval of the Application Owner.
8. Source codes shall not be accessible within the production environment.
9. Any Test or development environment/application must not be published to the external networks unless explicitly approved by owner and Information Security and necessary compensating controls are implemented.
10. Implementation of production applications shall only be done after proper testing, acceptance by the end users, and updates to the libraries that hold the source code.
11. All changes to libraries that hold operational code shall be logged.
12. Previous versions of changed applications must be saved to support a fallback scenario.
13. End users are not permitted to install unauthorized and / or pirated copies of software in to KGiS owned computer systems.
14. KGiS owned and licensed software shall not be loaded on an employee's personal computer system without authorization of the ISO and within the sphere of cover of the license agreement.
15. ISO shall review all the software installed in the computer systems and servers annually to ensure KGiS is in compliance with all its software license agreements with vendors.

12.10 Policy Area: Technical Vulnerability Management

12.10.1 Policy Section: Management of Technical Vulnerabilities

1. The operating system or environment for all Information System resources shall undergo a regular & periodic vulnerability scan.
2. The frequency of the vulnerability scanning shall be dependent on the criticality of the operating system and information system environment, the information system asset

classification, and the data classification of the data associated with the information system resource.

3. Vulnerability assessment (VA) scan shall be performed for all KGiS servers, storage devices, appliance, network and security devices at least once in 6 months.
4. Vulnerability assessment (VA) scans shall be performed for all endpoint systems at least once a year.
5. All external public IP's exposed to internet shall be tested as part of external penetration testing once in a year.
6. Critical internal and external Web application shall be tested once in a year.
7. All critical network and security devices configuration shall be reviewed at least once in a year on a sampling basis.
8. KGiS shall grant authorization to appropriate members of the Security Operations to conduct internal vulnerability scanning and penetration tests against the organization's computing, networking, telephony and other information resources.
9. Vulnerabilities in the operating system, Information System and other infrastructure components shall be evaluated in view of their business criticality and treated to minimize the risks associated with them.
10. All vulnerability scans especially those that may cause a system (or a Service on a System) to behave erratically shall be planned to cause no or minimum disruption. All scans shall be subjected to KGiS Change Management Process and shall have advance notification backed by coordination of efforts from all stakeholders.
11. Corrective action shall be taken to minimize the risk from identified vulnerabilities based on the criticality and the results will be discussed during management meeting.
12. Mutual SLAs shall be defined and agreed with respective teams and vendors, as applicable and followed with for the closure of identified vulnerabilities.

12.11 Policy Area: Information System Audit Consideration

12.11.1 Information Systems Audit Controls

1. KGiS Internal audit Office (IAO) shall perform periodic risk-based information systems audits as per annual Internal audit plan.
2. Information systems audit shall be performed as per KGiS Internal audit office policy, methodology and process.
3. Internal audit conducted by KGiS Internal Audit Team shall cover the requirements of implemented Integrated Management Systems (IMS).

13 Communications Security

13.1 Objective

To ensure the protection of information in networks and its supporting information processing facilities.

13.2 Policy Area: Network Security Management

13.2.1 Policy Section: Network Controls

1. ICT team shall maintain an up-to date Network architecture diagram that shall include all external and internal links, subnets, and all network equipment details.
2. All network connections shall be reviewed on an annual basis. Unjustified and unapproved network connections shall be disconnected and reported to the respective service owners and Information Security Office.
3. Network addresses used within KGiS network shall follow a formally defined schema which shall not be revealed outside the KGiS network.
4. Users shall only be provided with access to the IT services that they have been specifically authorized to use, in line with KGiS access control and Acceptable Usage policy.
5. All the network and security devices (i.e., routers, switches, firewalls, IPS, IDS etc.) shall be located in a physically secured area with limited controlled access.
6. No external devices/computers shall be allowed to be attached to KGiS network without following the KGiS Change Management process.
7. All network and security devices passwords shall be configured as per KGiS password policy.
8. The local passwords on network and security devices shall be stored in a secured manner.
9. The local passwords on network and security devices shall be encrypted and changed every 90 days.

13.2.2 Policy Section: Security of Network Services

1. All network equipment shall be stored in secured enclosed cabinet with locking facility.
2. Port Security or 802.1X Port authentication shall be used on all access ports. Unwanted or unused ports shall be disabled for all network systems.
3. Appropriate measures shall be adopted to ensure port security. Such measures include limiting the broadcast traffic on the port to a defined value, limiting the multicast traffic on the port, preventing LAN/ campus switching loops by avoiding loops in the LAN network, preventing auto-negotiated connectivity establishment between two switches to avoid DOS attacks, etc.
4. No wireless access points shall be attached to KGiS network without formal change management process. KGiS shall consider deploying and enabling wireless IPS to prevent rogue access points and other wireless threats.

5. Access to all external networks must pass through an access control point (i.e., IDS, IPS and firewall) before reaching any intended hosts, and shall be subject to authentication and authorization.
6. KGiS shall use various network controls such as firewall or Access Control Lists (ACLs) in order to restrict all types of network traffic that may enter or leave its network.
7. IDS/IPS profiles shall be implemented to protect and alert KGiS against internal and external attacks
8. Signature in the IDS/IPS profiles shall be reviewed, fine-tuned and configured based on the traffic directions and business requirements.
9. All network connected devices must be monitored proactively by Security Incident Event Management (SIEM) for timely detection of security breaches. In the event of any breach, KGiS's network operations team or designated ISO shall be immediately alerted.
10. All security events related to networks, security services shall be appropriately logged, monitored through SIEM.
11. All the network and security devices shall comply with KGiS Minimum Security baselines.
12. All the network and security devices configuration shall be reviewed at least once in a year on a sampling basis.
13. Network and security devices placed on all external network connections, shall be configured with a display banner message warning unauthorized use is prohibited.
14. All network devices and systems clocks in KGiS's network shall be synchronized with KGiS's NTP server or with approved external source (i.e., OEM timeservers).
15. Unwanted ports and services, configured on any network equipment, shall be disabled or blocked.
16. All unused connections and network subnets should be disconnected and disabled.
17. IT team shall be responsible to keep anti-virus, anti-malware and operating system security patches up to date at all times on their network equipment and systems.
18. Management of network and security devices shall be via only the management Interface. No production interfaces shall be used for the management of the network and security devices.
19. The usage of any tools that sniff or capture network packets, which may degrade the performance of the network shall have proper authorization from Information security office (ISO).

13.2.3 Policy Section: Network Availability and Maintenance

1. Quarterly checks shall be performed on network and security devices (e.g., components will be patched in a timely and proactive manner against published security vulnerabilities).
2. Network and security devices shall be appropriately managed and monitored on a daily basis by an authorized system/network administrator.

3. Only licensed software shall be used, and all the licensing information must be readily available in case of an audit.
4. Health of network and security devices shall be checked and monitored on a daily basis. The same shall include but not limited to CPU, Interface bandwidth, Memory, HDD, errors, warnings, etc.
5. Support contracts shall in place for all critical network and security devices.

13.2.4 Policy Section: High Availability and Backup

1. Failover mechanism shall be deployed when setting up all critical network and security devices, to avoid single point of failure that could cause the unavailability of the network and security services.
2. The configurations of all network and security devices shall be backed up as per the Backup Policy.

13.2.5 Policy Section: Standard Operating Procedures

1. Standard operational procedures shall be identified, documented for all critical network and security devices.
2. All equipment connected to the network must be configured according to documented procedure approved by designated personnel.

13.2.6 Policy Section: Identification, Authentication and Authorization

1. All network and security devices shall be integrated and authenticated through appropriate and approved Access Control Systems (ACS)/Access Control protocol.
2. Service accounts shall be configured with a password not less than 14 characters and change regularly as per password rotation policy set for privilege identities.
3. A separate privilege ID shall be used for the administrators, the same shall be different than that used for normal operations.
4. All the network and security devices administrators' access shall be reviewed once in 6 months.
5. Remote login to client network and security devices are only allowed over VPN and MFA.
6. Network and security devices shall be accessed and managed only by authorized administrators.
7. The complexity of administrator passwords for network or security devices shall comply with the KGiS's Password Policy.
8. Administrators shall be accountable for all the activities performed from any network and security devices using their login credentials.

13.2.7 Policy Section: Segregation of Network

1. Segregation or isolation shall be based on the value, classification and criticality of the service to the business and the information technology infrastructure.

2. De-Militarized Zone (DMZ) zone shall be implemented for all the services interfacing with internet and internal network.
3. Network Segregation and zone classification shall be periodically reviewed to ensure its effectiveness.
4. Controls shall be implemented to segregate various groups within the network by dividing them into separate logical network administrative domains and control traffic among these domains through premise router and firewall.
5. Systems containing highly sensitive information may be segregated—virtually or physically.

13.3 Policy Area: Information Transfer

13.3.1 Policy Section: Transfer Information through email

1. E-mails shall not be sent to public email addresses such as Gmail, Yahoo, and Hotmail etc.
2. All password(s) to encrypt documents shall conform to the Password Policy of KGiS.
3. All emails sent from KGiS to external organization shall include the standard disclaimer notice at the end of the email.
4. Employees shall exercise utmost caution while sending any email from inside KGiS to an external network.
5. All Information transfer by email shall be done in a way that complies with the KGiS's Acceptable Use Policy.
6. All password(s) required to open the encrypted attached file shall be transferred separately to the recipient either via a telephone call to an agreed number, or via SMS.
7. Email traffic shall be monitored for potential malware attacks through emails.
8. KGiS's emails shall not be configured to automatically forwarded to an external destination.

13.3.2 Policy Section: Transfer through Cloud Storage

1. **Cloud Upload:** It is strictly prohibited to upload KGiS's information on to public cloud or personal cloud sharing services such as OneDrive (personal), Dropbox, Google Drive, 4shared, etc. However, usage of KGiS OneDrive is permitted for official purposes.
2. **Cloud Download:** Download from public cloud drives are allowed, provided the same is from authentic sources and for business use only.
3. Official communication for any internal or external communication is through email, however in case use of email is not feasible/secure below ways shall be used.
4. **External File Sharing:** For sharing large files (i.e., greater than 10MB) with external parties and secure transactions, the users shall use only One Drive.
5. **Internal File sharing:** users can utilize below mechanisms to share documents internally
    a. Share folder
    b. One Drive

c. MS Teams

6. **External FTP File Upload:** File uploads to external FTP server shall not be allowed.

13.3.3 Policy Section: Transfer through portable storage devices

1. Removable media is prohibited from use in KGiS. Only Information Security approved users can use the removable media. (USB drive, Memory Card)
2. The users shall be responsible to safeguard and protect the removable media and portable storage devices used shall be password protected with a strong password as set out in KGiS's Password Policy.

13.3.4 Policy Section: Transfer through Internal Mail System

1. Mails sent through the internal mail system shall be clearly addressed to the intended recipient.
2. Files or documents containing controlled data shall not be transferred loose and shall be appropriately packaged, in a sealed envelope, to avoid disclosure to others or loss of information.
3. Any information transferred shall be relevant and be the minimum necessary for a specific purpose.
4. If information is deemed reasonably high risk if lost or misplaced, where possible this shall be hand delivered to the recipient.

13.3.5 Policy Section: Physical Media Transfer/In Transit

1. Physical media carrying sensitive information shall not be identified.
2. Only approved and recognized courier services provider shall be engaged for delivering the documents and couriers.
3. Labelling requirements for physical media carrying sensitive information shall be defined.
4. Physical media in transit carrying sensitive information shall be tracked sufficiently in accordance with the sensitivity of the information it contains.
5. All media transaction (issuance, revocation, movement) shall be recorded.

13.4 Policy Area: Electronic Messaging

13.4.1 Policy Section: Email Security

1. KGiS corporate email software system shall run and operate on a dedicated, redundant, deployable, and high availability server.
2. Any patches or upgrades to current known vulnerabilities on the email server software shall be applied as per the Change Management Policy of KGiS.
3. Vendor recommendations shall also be considered and applied on the email servers, while implementing the approved MSB.

4. SMTP, POP, IMAP and other service banners shall be reconfigured so that unauthorized persons will not be able to know the type and the version of the email server as well as the operating system.
5. Access to the email server application by the normal end users / unauthorized personnel shall be restricted.
6. KGiS approved Minimum Security Baseline (MSB) shall be implemented on Exchange servers.
7. Host operating system on email servers shall be configured to ensure that:
    a. Temporary files created by email server application are secured;
    b. Temporary files created by email server application are restricted to location (specific designated sub-directory) and access to a specified designated subdirectory.
8. Access to any temporary files created by email server application is limited to email server processes that created these files.
9. End users' mailboxes shall be installed on a different hard drive or logical partition other than the operating system and the email server application.
10. A limit on the end users' mailbox shall be set minimum of 5 GB. A limit on the maximum available size for Head of Departments and Directors mailboxes including Department mailbox shall be set to 10 GB unless there is an exception approval from Information Security.
11. A limit on the maximum available size of the KGiS Executive Management (C levels) mailboxes shall be set to 20 GB unless there is an exception approval from Information Security.
12. The size of attachments of incoming email from outside organization shall be restricted to 15 MB and that of outgoing external mail restricted to 10 MB unless there is an exception approval by Information Security Office.
13. When sending an email outside the organization, a maximum number of 200 email participants shall be allowed per email unless it is part of the employee's job function, with prior approval from information security, to send out large communication up to organization wide for example – change management, business continuity, and communications department.
14. The procedures for journaling, archiving and retaining the mailboxes shall be implemented.
15. A centralized virus scanner shall be implemented on either the Email Gateway, Firewall and / or Email server.
16. A content filtering device or software control shall be implemented and configured to block suspicious messages and notifying the recipients about the blocked message.
17. KGiS's legal disclaimer shall be added to all outgoing emails of KGiS.
18. End user mailboxes on the server must be included in the active backup, archival and recovery as per KGiS Backup Policy.
19. Ensure Domain Keys Identified mail (DKIM) shall be enabled on all exchange servers.
20. Ensure Sender Policy Framework (SPF) records shall be published on all exchange servers.

21. Ensure Domain based message authentication, reporting and conformance (DMARC) records shall be enabled on all exchange servers.
22. Ensure Security Incident Event Management (SIEM) solution shall be enabled on all exchange servers and security logs shall be reviewed by Security Operations team. Any suspicious activities correlated by the SIEM solution shall be notified as a workflow to Information Security office to mitigate and resolve as per incident classification and prioritization
23. Ensure Anti-virus, Endpoint Detection and Response and Anti-malware software shall be installed and scanned on all Exchange servers.

13.4.2 Policy Section: Email Network Protection

1. The Email server shall be located on the internal network and protected by a Firewall, or it shall be located in a Demilitarized Zone (DMZ).
2. KGiS shall ensure that a Firewall blocks all inbound traffic to the email server except if routed through the documented managed ports.
3. KGiS IDS / IPS shall be configured to monitor Email traffic, critical files, and system resources available on the email server.
4. Network Switches shall be used on email server network segment to protect against network eavesdropping.

14 System Acquisition, Development and Maintenance

14.1 Objective

To ensure that Information Security is an integral part of Information Systems across the entire lifecycle.

14.2 Policy Area: IS requirements analysis and specification

1. New proposed information systems as per the business requirement shall be authorized and approved by management.
2. Information Security Office shall perform Information and Business Continuity Risk assessment for all KGiS Information Systems during design and development phase/stage.
3. Any major risks identified during the risk assessment shall be addressed during the development stage. ISO shall re-validate the risks as per KGiS Information Security Risk management framework.
4. KGiS shall establish/ provide Information Security requirements for new Information Systems or major enhancements to existing Information Systems as part of its business requirements.
5. KGiS shall include Information Security requirements and/or security specifications, either explicitly or by reference, in Information System acquisition contracts, based on an assessment of risk.
6. The solicitation for Information Systems and services (e.g., Requests for Proposals) shall include, either explicitly or by reference, the Information Security requirements that need to be met in each one of the phases: Design and Development processes; Implementation; Operations and Management and Documentation.
7. Statements of business requirements for new services, or enhancements to existing services shall specify the needs for Information Security controls and resources.
8. Information Security requirements and controls shall reflect the business value of the Information Assets involved and the potential business impact that might result from an absence or failure of security.
9. High Level Design (HLD) documents or design documents shall be reviewed by Information security office.

14.3 Policy Area: Secure Application Development

1. Application Development team shall start developing codes for the Application/ Software's by considering the following activities:
    a. Designing the architecture of the proposed Application/ Software's taking into consideration, the requirements from users, technical and information security standards.

b. Data input to application/software shall be validated to ensure that it is correct and appropriate.

c. Data output from the application/software shall be validated to ensure correct processing of data.

d. Internal validation checks shall be incorporated into application/software to detect any corruption of the data processed.

e. Development team shall ensure that the Segregation of Duties (SoD) is in place for the data to be processed / generated.

f. Applications must identify and handle error conditions in an efficient manner.

g. Rules for checking the valid syntax of application/software inputs (e.g., character set, length, numerical range, acceptable values) shall be in place to ensure that inputs match specified definitions for format and content.

h. Requirements for ensuring authenticity and protection of message integrity in application/software shall be identified and implemented.

i. KGiS application minimum security baseline (MSB) shall be implemented.

j. Internal Integration requirements e.g., Active Directory, Security Incident Event Managements solutions etc.

2. Web Application Firewall (WAF) shall be enabled on block mode for the application published over the Internet.
3. SSL Certificate & Digital Certificate Authority shall be used for publishing the application.
4. Development, testing/QA and production environment shall be segregated to reduce the risk of unauthorized access or changes to the production systems as per the Segregation of Duties
5. Application and Database environment shall be segregated to minimize the risks of unauthorised access.
6. Any Test or development environment/application must not be published to the external networks unless explicitly approved by owner and Information Security and necessary compensating controls are implemented.

14.4 Policy Area: Security Testing

1. KGiS shall ensure perform security code review process is integrated into the Quality Assurance testing/review process.
2. Application/Software's shall be tested for the following security features (but not limited to):
   a. Authentication;
   b. Authorization;
   c. Confidentiality of data;

d. Integrity checks;

e. Input validation checks;

f. Processing security controls; and

g. Output security controls

3. Any Information system/application/ mobile application shall be subjected to security testing before deployment in Production environment as part of operational readiness procedure.
4. KGiS shall conduct web-application security testing for Public facing application before moving to production to ensure all developed application/software's complies with KGiS's Information Security policies.

14.5 Policy Area: User Acceptance Testing (UAT)

1. Acceptance criteria and requirements for new/updated Information Systems shall be established, with suitable tests of the system carried out prior to acceptance and prior to placing them in the operational environment.
2. Information security controls implementation in accordance with the Security criteria as well as KGiS information security policy shall be tested and reviewed by ICT team and approved by information security office.
3. All manuals and materials provided to end users while implementation or upgrading Software shall have service owner's approval.
4. End user shall complete appropriate training before using a new business application or a new version of the existing business application programme.
5. User acceptance testing shall be carried out before deploying the new developed / enhanced / purchased information system into production.
6. Any security and ICT risks identified shall be communicated to Information security office to register and document the risks.

14.6 Policy Area: Source Code Access and Security

1. Access to Information systems storing the source codes shall be restricted to authorized users as per role-based access.
2. Access to the source code libraries shall be reviewed periodically.
3. Escrow agreement shall be incorporated on the contract if the source code is owned and managed by the external developers.

14.7 Policy Area: Change Management Process

1. Changes to the application/software development or enhancement shall be controlled through KGiS's change management process.

2. Access to the application/software environment shall be granted according to SoD matrix to avoid conflict of interest.

14.8 Policy Area: Technical review of applications after operating platform changes

1. All changes shall be performed as per KGiS Change Management process.
2. Testing for all applications shall be carried out in a test environment when operating systems are changed including the patches and configurations.

14.9 Policy Area: Maintenance and Support Contract

1. Contract shall be in place with the OEM or vendor for critical application supports.
2. SLA shall be signed with the vendors and periodic service reports shall be submitted to business owners/service owners.

15 Supplier Relationship

15.1 Objective

To ensure protection of KGiS assets that is accessible by suppliers.

15.2 Policy Area: Information Security Policy for Supplier Relationship

1. All the third parties required physical and logical access to KGiS premises shall be provisioned based on the approval from ISO for logical access and HR Administration department for physical access and office space.
2. All Third-Party access to KGiS Information Systems, Local Area Network (LAN), Wide Area Network (WAN), and Wireless Access Infrastructure shall have formal authorization.
3. Risk assessment shall be conducted to identify potential risks to KGiS as a result of a Third-Party access.
4. These risks shall be appropriately controlled or mitigated through effective controls that need to be implemented to regulate and monitor the Confidentiality, Integrity and Availability of the Information processed by the Third Party.
5. The assessment of risks related to Third Party access shall consider the following aspects as mentioned in the KGiS Information Security Risk Management Methodology:
    a. Possible impacts to the controls of the Information processing facilities involved.
    b. The classification of the Information assets.
    c. Processes for identifying, authorizing, authenticating and reviewing access rights of the external parties.
    d. Security controls to be used by the external party when storing, processing, communicating, sharing or exchanging Information.
    e. Possible impact to both parties resulting from assets being unavailable.
    f. Prior to authorizing access to external parties to Information and Information Systems, Service Manager(s), Information Owners and Information Custodians shall confirm that:
        - The Terms and conditions of access are documented (e.g., Service Level Agreement (SLA), Contracts, Non-Disclosure Agreements, and Memorandum of Understanding (MoU) etc.).
        - Responsibilities for managing and monitoring the external party access have been assigned and documented; and
        - Security Controls have been implemented and tested against identified risks.

15.3 Policy Area: Addressing Security within Supplier Agreements

1. Third Party access to KGiS Information Systems shall be provided based on a formal contract and Non-Disclosure Agreement (NDA) between KGiS and the Third-Party service providers.
2. At a minimum, contracts with Third Party service providers for provision of Third Party's access to KGiS Information Systems or for processing on KGiS information at its location shall include [minimum information security requirements set by the Business owner in consultation with the Legal Department] OR [Information Security Office] & controls along with confidentiality and Non-disclosure clauses. The business owner shall be responsible for ensuring minimum information security requirements are set in the services specification, statement of work or other technical document.
3. Outsourcing contracts shall include the following conditions in accordance with generally accepted industry practice at a minimum:
    a. The level of physical and logical security that shall be provided to maintain the Confidentiality and Integrity of KGiS Information/data processed.
    b. The expected security level & SLA of the provided service and the level of Availability in the event of a disaster.
    c. Provision for Confidentiality, Non-Disclosure and Acceptable Use relating to the Information/data processed by the outsourced function or service.
4. A defined process for Service Delivery along with different roles and responsibilities shall be documented and updated periodically or after any significant change occurs, by the respective business function utilizing the third-party services.
5. KGiS shall have the right to review and audit (on the ground) compliance with the Terms of the Outsourcing Contract.

15.4 Policy Area: Monitoring and Review of Supplier Services

1. Manager shall maintain appropriate reports and records, to monitor and measure its compliance with the Information Security requirements as documented in the Service Delivery agreements with the Third-Party providers.
2. Changes to Information Systems developed by Third Party service providers shall be documented and controlled.
3. Review and resolution report on the any Information Security incident at the Third Party shall be report to KGiS ISO to avoid any possible risk to Organization infrastructure or Information.
4. ISO shall review and monitor the security practices and processes of the supplier on a regular basis.

5. Security controls compliance of Third-Party service providers of Information System services shall be monitored.

15.5 Policy Area: Managing changes to Supplier Services

1. Procurement shall periodic monitor and update the changes to the supplier.
2. For critical suppliers, KPIs shall be created and monitored by supplier relationship managers on annual basis. Results of KPI monitoring shall be considered by procurement as part of contract renewal/termination of suppliers.
3. Regular reports shall be provided by suppliers to enable supplier relationship managers to:
   a. Ensure supplier is meeting current business requirements (KPIs) and is continuing to adhere to the contract agreements and service level agreements
   b. Ensure supplier performance is competitive with alternative suppliers and market conditions.
   c. Identify and mitigate risks relating to supplier's ability to continue effective service delivery in a secure and efficient manner on a continual basis.
4. The terms of formal agreements shall be reviewed periodically according to business needs.
5. When the contract is changed or terminated, the access rights for employees of suppliers must be removed according to "Access Control Policy". Further, when the contract is changed or terminated, Department must ensure that all the equipment, software or information in electronic or paper form is returned or destroyed.

15.6 Policy Area: Cloud Computing Policy

15.6.1 Policy Section: Cloud Computing Usage and Storage

All Cloud service providers (Public, Private and Hybrid) shall comply with this Cloud Computing Policy and applicable India laws and regulations.

1. Use of Cloud computing services for work purposes must be formally reviewed and authorized by Information Security Office (ISO) based on the critical of the data, storage, outcome of risk assessment, if required Legal and Compliance approval shall be obtained based on the impact and criticality of data and systems.
2. The ISO shall verify whether security, privacy and all other technical related controls and requirements are adequately addressed by the Cloud Service Provider (CSP).
3. CSP shall ensure that the above requirement is met by the sub-contracted data processor with sufficient documents to support the claim.
4. The use of Public Cloud services shall comply with applicable INDIA regulations, KGiS Information Security Policy and relevant cloud security controls Policy Section: Cloud Service Provider Agreements.

5. All CSP agreements for hosting our services on Public Cloud services shall be reviewed and approved by Legal and compliance. KGiS Internal audit Office (IAO) shall perform periodic risk-based information systems audits as per annual Internal audit plan.
6. At a minimum, the following information security requirements shall be incorporated within the CSP agreement:
    a. Information security risks and mitigation;
    b. Data protection, storage and security controls;
    c. Information security incident management;
    d. Disclosing the sub-contractor's information involved in processing (Storage, Monitoring, Handling. etc) our data;
    e. No ownership rights on the stored data regardless of the format or storage medium.
    f. Data portability measures; and
    g. Change, Recovery and Restoration.
7. CSP shall inform KGiS's if any data disclosure request is made by any authorities, so that the KGiS's has the ability to object to such disclosures.
8. CSP shall get consent from KGiS if any changes with respect hosting location (i.e., system or system components) where the information resides.

15.6.2 Policy Section: CSP Data Management Controls

1. ISO shall review and approve the Security and Business Continuity controls in the high-level diagram with security architecture and deployment model.
2. ISO shall validate that adequate controls are implemented by CSP, addressing KGiS's requirements for periodic testing of the continuity and disaster recovery plans and timely communicating the outcome of results to KGiS.
3. ISO shall request Information Security and Business Continuity assurance reports (for example SOC2, Penetration Testing, Vulnerability assessment reports) to ensure all compliance & contractual requirements are met.
4. CSP shall ensure adequate controls are in place for secure disposal and it shall also guarantee that KGiS' s data cannot be recovered by any technology or process after the disposal.

15.6.3 Policy Section: Access Control

1. CSP Administrator activities shall be logged across all the servers, devices, etc. and reviewed periodically.
2. CSP administrator access shall be reviewed at least Half-yearly.
3. Cloud administrator access shall be approved by the CSP and maintain appropriate records.

15.6.4 Policy Section: Segregation of Network and Tenants

1. CSP shall ensure KGiS's information services, users, network, databases and applications are segregated logically and physically between different tenants.

16 Information Security Incident Management

16.1 Objective

To ensure effective management of Information security incidents from the time it is reported also provide guidance to employees on proper response to, and efficient and timely reporting of security related incidents.

16.2 Policy Area: Management of IS Incidents and Improvements

16.2.1 Policy Section: IS Incident Management Responsibilities and Procedures

1. KGiS shall develop an Information Security Incident Management Process which shall outline different phases from reporting or detection till resolution and documentation of Information Security Incident.
2. KGiS shall establish an Information Security Incident Response Procedure / outlining the formulation of the Information Security Incident Response Team (ISIRT) including defining the roles and responsibilities associated with each team member and developing the corresponding ISIRT procedures to ensure a quick, effective and orderly response to Information Security Incidents.
3. Reporting Team (ICT Service Desk / Security monitoring team) shall classify and categorize incident based on the business impact and the urgency of incidents as defined in Security Incident Management Process
4. Security Operations team/Information security Office (ISO) shall reclassify the incident (if needed) based on the impact and severity and update problem manager which in turn shall involve ISIRT team if the incident is severity 1.
5. ISO shall determine to which level of the organization initial communication is required, what constitutes the content of the communication, and how best to distribute or deliver the communication.
6. ISO shall communicate with relevant parties to do containment and eradication of the incident.
7. Information security incident shall be contained and resolved using the appropriate documented security incident response procedure.
8. ISO shall communicate back with reporting entity and seek confirmation on closure.
9. In the case where law enforcement is involved, KGiS Contract and Legal Department and Information Security Office will act as the liaison between law enforcement and KGiS.
10. ISO shall continuously monitor the defined timelines for reporting and resolution of the open and in-progress incidents and periodically report to the management on overall status.

16.2.2 Policy Section: Reporting Information Security (Events and weakness)

1. Any personnel using KGiS Information resources shall report suspected hardware or software security incidents to his/her supervisor / Information security office and/or ICT Service Desk.
2. All KGiS employees, contractors and third-party users shall be made aware of their responsibilities to report any Information Security Incident as quickly as possible.
3. Any spam or suspicious email shall be forwarded to reportspam@KGiS.com
4. If Sensitive or Confidential Information is lost or is suspected to be lost or disclosed to unauthorized parties, the end user shall notify ISO immediately.

16.2.3 Policy Section: Assessment of Security Incidents and Categorization

1. The ISIRT shall analyse and investigate the incident to reduce the likelihood or impact of future incidents.
2. Information Security office and Incident Manager shall review the incident and if need arises shall re-categorize and re-classify the incident.
3. Incident manager shall update necessary stakeholders based on the criticality of the incident
4. Any communication to be shared with the external stakeholder shall be routed through Contract and Legal Dept. and communicated by the Marketing and Communications team.

16.2.4 Policy Section: Response to Information Security Incidents

1. Security Incident response plan shall have the following phases
   a. Incident containment;
   b. Incident Analysis;
   c. Incident Resolution;
   d. Incident Resolution testing;
   e. Incident Implementation; and
   f. Incident Documentation & Report;
2. After security incident resolution, root cause for the incident shall be analysed (for high severity incident such as P1 and P2) and necessary actions shall be taken to avoid such incidents in future.
3. Security Incident report shall be documented by ISO and submit the same to the management.
4. HR shall be notified immediately for all potential breaches that resulted as Security incidents to take necessary disciplinary action.
5. Any organizational level incident which interrupts complete operations of the business shall be managed in accordance with business continuity and IT disaster recovery plans.

16.2.5 Policy Section: Testing of Incident Response

1. Internal Incident response test shall be performed at least once in a year to test the effectiveness and efficiency of Security Incident Response Plan.
2. Testing plans and cases shall be developed to validate the effectiveness and usefulness of its incident response capability.
3. Expected test results shall be defined and documented.
4. Incident response capability testing shall be conducted, and the outcome shall be compared to the expected results to identify gaps and weaknesses for remediation.

16.2.6 Policy Section: Training on Information Security Incident Response

1. An incident response training program shall be established.
2. The training program shall be designed based on the target audience and shall be customized to end users, system administrators, and incident responders.
3. The training program shall cover all incident response procedures and their respective users.
4. The lessons learnt from the past incidents shall be used as reference in training ISIRT and related teams.

16.2.7 Policy Section: Learning from Information Security Incidents

1. The lessons learnt such as root cause, handled & containment strategy and corrective shall be documented and implemented to avoid similar incidents in the future.
2. Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
3. Detailed Information of security incident shall be recorded to facilitate knowledge base and lesson learned in order to identify additional control to avoid similar incidents in future.

16.2.8 Policy Section: Collection of Evidence

1. Relevant Information and data before, during and after information security incident shall be identified, documented and practiced.
2. Evidence collected during the security incidents investigation and analysis shall be stored and protected as per applicable laws and jurisdiction requirements of INDIA.

17 Information Security Aspects of Business Continuity Management

17.1 Objective

To ensure that Information Security shall be embedded in the KGiS business continuity management systems.

17.2 Policy Area: Business Continuity Management

17.2.1 Policy Section: Business Continuity Management Responsibility

1. KGiS Management shall have an overall responsibility for developing and implementing a Business Continuity Management (BCM) Program.
2. KGiS shall identify/nominate a BCM Coordinator / Manager to carry-out the Business Continuity activities as per the BCM Program.
3. KGiS in cooperation with respective business unit owners shall establish an IT Continuity Framework (comprising of Disaster Recovery Plan and System Specific Recovery Procedures) for supporting the Information Systems continuity requirements of the organization.
4. Each business unit of KGiS shall have the primary responsibility for planning, development, maintenance, and testing of its respective unit and shall assist the BCM organization and the Senior Management in the development, implementation and management of KGiS Business Continuity Plan (BCP).

17.2.2 Policy Section: Business Continuity Management Process

1. KGiS Management shall develop, design and implement formal BCM Process.
2. BCM Process shall take into account the various criteria and controls as required by the ISO 22301 Standard for BCM.
3. The BCM Process shall take into account the availability requirements – Recovery Time Objective (RTO) and recovery requirements – Recovery Point Objective (RPO) for all critical services of KGiS.
4. KGiS shall ensure that a Business Impact Analysis (BIA) and detailed Risk Assessment are conducted to reflect the criticality of various services as well as risks related to the services is identified.

17.2.3 Policy Section: Development and Implementation of Business Continuity Plan

1. A BCP shall be developed to maintain and restore business operations in required time scales following interruption to or failure of critical business processes. The plan shall also include the Disaster Recovery Plan (DRP).
2. KGiS shall establish alternative Disaster Recovery Site (DRS) with all required facilities and infrastructure to ensure recovery of services is performed within the defined RTO.

3. KGiS shall ensure that the IT Continuity Plans is safeguarded against unauthorized disclosure and modification; sections of the plan shall be distributed only on need-to-know and need-to-use basis.

17.2.4 Policy Section: Information Systems Continuity Planning Framework

1. KGiS shall develop a comprehensive framework for Information Systems Continuity/ Disaster Recovery Planning to ensure that it is in line with the Corporate BCP and Strategic IT Plan to ensure consistency and to guarantee that maintenance and testing are prioritized.
2. KGiS shall ensure that Information processing facilities are implemented with redundancy sufficient to meet availability requirements. Redundancy/Failover testing shall be conducted for the critical systems/applications to ensure the compliance and continual sustenance of the implemented controls.

17.2.5 Policy Section: Testing, Maintaining and Re-assessing the Plans

1. KGiS shall develop a detailed BCP Testing methodology as per the leading practices and standards and shall periodically test the BCP.
2. The BCPs shall be reviewed and updated at least once in a year by KGiS to reflect the change in business arrangements (e.g., acquisition of new equipment, change in personnel, change in operational system etc.) and to ensure that the plans are valid and effective during adverse situations.
3. A formal change procedure shall be developed to ensure that only authorized personnel shall update plans and all the required changes are incorporated in the plan.
4. KGiS shall ensure that concerned Employees receive regular training regarding the procedures to be followed in case of an incident or a disaster.

18 Information Compliance

18.1 Objective

To identify, monitor and comply with INDIA Information/Cyber Security & Data Security laws that are applicable to KGiS.

18.2 Policy Area: Identification of Applicable Legislation and Contractual Requirements

1. The Legal Department shall provide continuing guidance on all applicable laws and regulations in the INDIA which apply to information security, data protection and business continuity, including all changes in applicable law and regulation from time to time. Such guidance shall be communicated to Information Security Office (ISO) for onward coordination on implementing any necessary changes.
2. The Legal Department shall also document specific contractual terms in each contract relating to information security, data protection and business continuity as required by applicable laws and regulations or which are prudent in the view of the Legal Department after consulting the business team, but the applicable business team shall be responsible for the technical content of statements of work relating to specific operational requirements relating to information security, data security and business continuity. Consideration will be given to the ability of KGiS to commercially achieve in negotiations the desired technical outcome.
3. The applicable business owner/team shall be responsible for implementing KGiS's obligations arising from the Legal Department's advice or from contractual terms agreed with business partners (subject to inspection or auditing by internal audit and the interpretation and guidance of the Legal Department).
4. The KGiS Legal Department and ISO shall engage representatives from key parts of the organization affected by revised or new legal or regulatory requirements. Any changes needed based on revised or new legal or regulatory requirements must be reflected in this policy and standards as necessary.
5. The Legal department shall include clauses in relation to information security that it considers prudent within the standard contract templates used in KGiS, save that services-specific information security requirements on each transaction are included in the relevant services specification or statement of work by the applicable business team with ISO input as required. Typical minimum contractual clauses shall include the following:
    a. Non-Disclosure statements;
    b. KGiS rights to audit for compliance and security breaches (subject to negotiation strength);
    c. Intellectual Property rights; and
    d. Data Protection.

6. ISO shall suggest any changes to contractual templates to reflect Information Security requirements, to the extent these need to be included in contractual templates (as opposed to technical documents such as statements of work or information security schedules to within contracts, which will be subject to legal review).

18.3 Policy Area: Intellectual Property Rights

1. Software, Systems or Documents that an employee develops within the scope of his/her employment with KGiS, using KGiS resources, machines or data, or on KGiS time, shall be the Intellectual Property of KGiS unless a written and legal agreement states otherwise. The employee agrees to vest all such Intellectual Property (including moral rights) in KGiS or its relevant affiliate and shall do or sign all such documents necessary to do complete such transfer.
2. Management shall ensure that all employees providing such programs or documentation are aware of the Intellectual Property restrictions mentioned above and that a statement to this affect is to be incorporated in individual's Employee contracts.
3. Employees must not sign any Non-Disclosure agreements (NDAs) or other legal or commercial agreements provided by third parties without the advance authorization of KGiS Legal Department (and even in such cases, an authorised signatory according to the DOA will sign such documentation).
4. Only license software's shall be installed and used as per license agreement. Each business owner who deploys licences shall follow the procedures for monitoring licensed usage and remaining within contractual deployment limits, as set by ISO.

18.4 Policy Area: Protection of Records

1. KGiS shall define a process to identify and protect important records from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
2. KGiS shall determine specific system requirements resulting from the identified requirements and define specific security and business controls to ensure all record protection requirements are met.
3. KGiS shall periodically review requirements and associated controls for completeness.

18.5 Policy Area: Protection of Personally Identifiable Information

1. KGiS is committed to compliance with applicable data privacy laws and with data privacy provisions in its contracts with employees and third parties.
2. KGiS maintains and shall ensure that its contractors maintain, appropriate and reasonable security measures against unauthorized or unlawful processing of Personal Information or its accidental loss, destruction or damage, and to detect and respond to data security or data privacy breaches.

3. KGiS's customer contracts will establish the allocation of roles and responsibilities with respect to data privacy and will require customers to comply with their obligations under applicable data privacy laws.
4. KGiS will obtain and process Personal Information fairly, lawfully and securely. KGiS will ensure that Personal Information will be collected, processed and used for limited, specifically stated purposes, in a way that is adequate, relevant and not excessive.
5. KGiS and its personnel will not disclose Personal Information to any third party with whom KGiS is not entitled to share that information. KGiS will enable the updating of Personal Information as necessary, and ensure personal information is kept for no longer than is necessary.
6. KGiS is subject to applicable data privacy laws of the INDIA, where it is based, and may in respect of certain of its services, also be subject to applicable data privacy laws of the countries in which its customers are based.

18.6 Policy Area: Regulation of Cryptography Controls

Any cryptography controls are employed within the information system, the system should perform all cryptographic operations (including key generation) as per INDIA cryptographic controls as applicable.

18.7 Policy Area: Independent Review of Information Security

1. KGiS shall ensure that independent audits and gap analysis for policy compliance are performed on an annual basis, or as otherwise necessary (i.e., significant infrastructure or application upgrade or modification) to ensure compliance with security policies, standards, procedures and other documented security requirements.
2. KGiS should ensure that an independent entity, other than the Business Owner, Security Operations, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts vulnerability assessments and penetration testing of the critical information system.

18.8 Policy Area: Compliance with Security Policies and Standards

Compliance with Information Security policies and procedures shall be included in all employee and vendor contracts and agreements.

18.9 Policy Area: Technical Compliance Review

1. KGiS shall define and execute a process for routine checking for technical compliance with security standards.
2. Security Operation shall perform periodic vulnerability assessment and penetration testing as per agreed Information security plan.

3. ISO shall perform periodic MSB/ technical compliance review on all critical information systems as per defined information security plan.
4. KGiS shall ensure results of compliance checking is performed by, and the results are reviewed by authorized personnel with adequate technical capabilities.
5. Report any issues detected during technical compliance checking to the appropriate authority for remediation.