FIVE ▶

INFORMATION SECURITY POLICY

Issued by the Senior Director of Cyber Security
Approved by the Board, Jan 2021

Document Information:

Document Title:		Information Security Policy				
Version no	**Description**	**Date**	**Proposed by**	**Reviewed by**	**Approved by**	**Remarks/Changes proposed**
1.0	First Release	10-01-2022	Sujith Sidharthan	Sinto Neelankavil, Vivek Srinivasan	Jaydeep Anand	First release approval

Content:

Contents

1. Introduction

FIVE Holdings (BVI) Limited (hereinafter referred to as "FIVE") Information Security Policy is an integral part of the FIVE IT policy landscape. This policy should be read in close conjunction with the FIVE IT procedures. The Information Security Policy defines the capabilities and requirements to protect information and systems from unauthorized access, use, disclosure, disruption, modification, data loss or destruction. This is accomplished through organizational and technical measures in accordance with business requirements and relevant laws and regulations.

This Information Security Policy constitutes the commitment of FIVE's management to take responsibility for achieving an organization-wide level of information security and setting a baseline for the information security controls that shall be applied by FIVE Holdings (BVI) Limited.

Each information technology system must be engineered towards the goal of a holistic, integrated security approach to serving the mission of the organization. In support of this, FIVE will achieve its information security objectives by continuously identifying, assessing, eliminating, or otherwise treating information security risks.

2. Objectives

The Information Security Policy's primary objectives are as follows:

- **Integrity:** Business and external stakeholders can rely on FIVE data.
- **Reliability:** To prevent Information security related events from affecting FIVE's business.
- **Confidentiality:** To protect Information and its information processing assets from unauthorized disclosure or access.
- **Availability:** FIVE ensures that all relevant information included in the policies, procedures and other vital templates are available when required.
- **Compliance:** FIVE ensures compliance with legal and regulatory requirements.

To ensure the policy's purpose, an Information Security Management System is implemented to:

- Demonstrate the organization's commitment to establish information security by establishing comprehensive security processes throughout the organization.
- To convey management's mission and vision for incorporating Information Security into the Organization's culture
- To identify groups/ teams and individuals responsible for implementation, maintenance, compliance, and improvement of Information Security
- To establish requirements for FIVE users to understand and adhere to Information Security Policies and Procedures.

3. Scope and Applicability

The information security policy applies to all employees, third-party service providers, and contract employees of FIVE (hereafter referred to as "users"), and clients/ customers visiting FIVE who engage in work and have access to FIVE's information or information processing facilities. Information technology will also act as an enabler in implementing information security controls across the organization.

3.1 Coverage

The Policy and procedures contained in this document have been established to cover information / data, software, hardware, networks, and information processing facilities used by FIVE at all its locations.
More specifically, the Policy applies to, but is not limited to, the following information assets,

- All proprietary information
- Personal information relating to employees
- Personal information relating to customers
- Inquiry details made by prospective guests
- Personal information relating to contractor employees
- All hard-copy documents
- All software assets such as application software, system software, and utilities
- Websites, portals, and other information systems
- All physical assets, such as computer equipment, network, and communications equipment

4. Responsibility

This policy defines the authority, roles and responsibilities of Information Security and the personnel responsible for protecting FIVE resources.

The information security organization structure at FIVE shall consist of:

- Security Steering Committee (SSC)
- Group Director - Cybersecurity
- IT Security Compliance Officer
- Senior Management

Responsibilities of the information security organization structure are as follows:

- **Security Steering Committee (SSC)**

  Participants: Group Director – IT, Group Director – Cybersecurity, CFO & COO, and select Head of Departments

  Key responsibilities:

  - Lead the Information Security program
  - Plan and conduct internal Audits
  - Monitor the information security related activities of the FIVE Properties
  - Suggest improvements to the existing processes

  Mode of Operation:

  - The SSC along with the Group Director – IT and Group Director – Cybersecurity must meet or have a conference call/video conference quarterly
  - The agenda and minutes of all the meetings should be documented and circulated to the members of the Security Steering Committee

- **Group Director – Cybersecurity**

  - The Group Director – Cybersecurity is responsible to ensure enforcement of the Information Security Policy at FIVE.
  - Lead the Security Steering Committee (SSC) and information security initiatives within the organization
  - Take necessary measures to maintain or implement security of the information systems
  - Ensure that the organization staff is adequately trained to meet the security requirements of the organization
  - Authorize new security products to be implemented across the organization.
  - Coordinate with the Head of Departments on new security initiatives
  - Ensure that the responsibilities are defined and that procedures are in effect to promptly detect, investigate, report, and resolve Information security incidents within the organization
  - To initiate appropriate measures to ensure the implementation of security measures at the Data center and other related information system resources
  - Approval of the necessary changes to the information security policies and procedures as recommended by the SSC.
  - Conduct periodic awareness of the implemented policies at the properties within the business
  - Interact with third-party organizations providing services specifically to the properties within the individual businesses to communicate Information Security requirements

- **IT Security Compliance officer**

  - The IT Security Compliance officer will be responsible for the implementation and compliance with security policy

and procedures within the organization and by FIVE users within their respective areas of responsibilities

- Maintaining a level of security awareness among the FIVE users through information security trainings
- Ensuring that sufficient controls are present to protect the confidentiality, availability, and integrity of the data
- Classifying the information and identification of specific information which should be treated as confidential

- **Senior Management**

  - Supporting the goals and principles of Information Security in line with Information Security strategy and objectives.
  - Actively supporting security through clear direction, demonstrated commitment and enforcement of Information Security.
  - Providing resources and budget for Information Security initiatives.

5. Information Security Policy Principles

The Information Security Policy is supplemented with procedures and processes documents for providing further details on the mandated implementation or required information security controls

5.1 Compliance to Information Security Policy

- IT team shall be responsible for the implementation and compliance of the Information Security Policy within their respective areas of responsibility.
- Mechanisms shall be established to ensure that all users also comply with the approved Information Security Policy.
- Legal and Compliance teams shall be responsible to identify legislation applicable to IT systems (e.g., data privacy) and assess their impacts as well as reviewing the legislation regularly.

5.2 Policy Review and Approval

This policy document shall be reviewed at least annually by the Group Director – Cybersecurity or in event of any significant changes (i.e., change in operations, change in technology, regulatory changes, and major security incidents) in the existing information security environment affecting policies and procedures. The Group Director – Cybersecurity will be responsible for making the changes to the policy and procedures and the same will be approved by the SSC.

All changes to the policy shall be communicated by the Group Director – Cybersecurity to senior management and users through appropriate forums and communication channels

5.3 Information Security Policy Documentation

- Information security policies and procedures shall be maintained and communicated to all users
- Information security documents such as policies, procedures, processes, security controls, and their implementation shall be securely (physically and logically) stored and available at a centralized location and made available, for reference at all times

5.4 Exceptions

- Approval for exceptions or deviations from the policies, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception approved by the Group Director – Cybersecurity
- Exceptions will not be universal but will be agreed upon on a case-by-case basis, upon official request made by the information asset owner. These may arise, for example, because of local circumstances, conditions, or legal reasons existing at any point in time.
- Exceptions to the Information Security Policy may have to be allowed at the time of implementation of these policies and guidelines or at the time of making any updates to this document or after implementation when the need arises.
- All exceptions during implementation must be submitted by Local IT representatives/ IT Helpdesk to the Group Director – Cybersecurity
- All approved exceptions or deviations must be recorded and managed in the exception tracker and reviewed on an annual basis by the SSC.

5.5 Auditing

The audit plan covers the assessment based on a test of the design and effectiveness of the Information Security Management System (ISMS) and the implemented security controls

5.6 Performance and reporting

- The Information Security exposure, risks, performance, and incidents must be reported to the SSC on an annual basis
- Based on these reports, management is responsible to take corrective actions where required and provides resources and budget for the same.

5.7 Association with Local Authorities and Special Interest Groups

- Contacts with law enforcement authorities, regulatory bodies, supervisory authorities, and other authorities shall be identified by the Legal & Compliance team & Cybersecurity Team

- Contacts shall be maintained with special interest groups and authorized information security forums (e.g., ISO, NIST, Gartner etc.) for receiving and distributing updates on new vulnerabilities, security and continuity threats, regulations and/ or information risks impacting FIVE

6. Organization of Information Security

The organization of information security establishes a management framework to initiate and control the implementation and operation of information security within the organization

6.1 Internal Organization

- The information security roles and responsibilities shall be defined and assigned at all levels ensuring that the individuals understand them.
- The duties and areas of responsibilities of users shall be segregated and records of the same shall be maintained to reduce the opportunities for unauthorized or unintentional modification or misuse of the information assets.
- In cases where segregation of duties is not possible, approval of the respective Head of Department (HOD) shall be obtained prior to allocating responsibilities to the employee/ organization. Also, appropriate compensatory controls such as monitoring of activities, audit trails, management supervision and independent reviews shall be implemented.
- All processes must adopt the principle of segregation of duties to the maximum extent possible. The initiation of an event must be separated from its authorization. The following principles must be followed:
  - Persons involved in operational functions must not be given additional responsibilities in system administration processes and vice versa.
  - Persons involved in testing processes must not be given additional responsibilities in system administration processes and vice versa.
  - The responsibility for performing a security review of the system or process shall be completely independent of the roles and responsibilities for developing, maintaining, and using the system or process
- Contacts with law enforcement authorities, fire department, emergency services and service providers shall be maintained by the Hotel Manager and/ or Security head. The contact details of these agencies should be maintained and displayed at office locations such as IT rooms, conference rooms etc. that are accessible to users.
- The Group Director – Cybersecurity shall maintain appropriate contact with special interest groups and authorized information security and data privacy forums for receiving and distributing updates on new vulnerabilities, security and continuity threats, regulations and/ or risks.
- New and upcoming projects and their management shall be aligned with the information security requirements of FIVE.

6.2 Teleworking

(**Refer:** FIVE Information Security Policy: Access Control: Remote Access Management & Teleworking)

7. Human Resource Security

The purpose of this policy is to ensure that users are aware of information security threats and concerns, their responsibilities, and liabilities; and are equipped to support the company's Information Security policy in the course of their normal work, and to reduce the risk of human error. (**Refer:** FIVE Human Resource Security Procedure)

- Job descriptions shall include information security roles and responsibilities of users from the IT and Cybersecurity Teams
- If required, screening and background verification shall be completed for users before on-boarding, in accordance with applicable laws and regulations
- Employment contracts shall include confidentiality and information security clauses that state the employee's responsibilities and obligations
- Management shall ensure that the importance of information security is communicated to all users via various channels
- Formal information security training shall be imparted to the users at the time of their induction.
- All users shall receive appropriate training on organizational policies and procedures, including security requirements, legal responsibilities, and other business controls as well as training in the acceptable use of information processing facilities e.g., logon procedure, software privileges etc.
- Formal disciplinary process shall be defined and enforced for all users who are found to be in violation of the information security policy, procedures, and their information security responsibilities
- The HR function shall formalize and document a termination process including the return of all issued assets such as equipment, access cards and/ or any other asset that is the property of FIVE to the IT Team.
- Revocation of assigned access rights and sign-off on the return of assets shall be obtained prior to the separation of the employee from the organization

8. Asset Management

- An asset management procedure (**Refer:** FIVE Asset Management Procedure) shall be developed, distributed, maintained, and adhered to comply with the asset management policy
- An inventory of information assets supporting FIVE's business processes shall be identified, recorded, and maintained for all assets across locations
- All identified information assets shall be assigned an 'asset owner' and 'asset custodian'

- Responsibilities of the asset owner and asset custodian shall be defined **(Refer:** FIVE Asset Management Procedure: Roles and Responsibilities)
- Information asset criticality value shall be determined based on the CIA criteria defined in the Information Asset Management Procedure (**Refer:** FIVE Asset Management Procedure: Data Classification Standards)
- Information asset inventory reconsolidation shall be performed on an Annual basis
- Information assets shall be classified and labelled (physically and logically) in accordance with the Data Classification Standard (**Refer:** FIVE Asset Management Procedure: Data Classification Standard)
- Information assets shall be protected against unauthorized access, misuse, and corruption, when at rest and in-transit
- All users shall return all the FIVE assets in their possession upon termination of their employment, contract, or agreement
- Information assets shall be sanitized to remove any classified information before being assigned for reuse
- Obsolete or retired assets shall be safely and securely disposed of in line with FIVE's Asset Disposal process (**Refer:** FIVE Asset Management Procedure: Media Handling: Disposal of Media)
- Information asset register shall be updated after the disposal of information assets
- All employee and third-party staff carrying media are required to ensure its appropriate protection during transit
- Hard disk drives sent for recovery purposes shall be transported using only the services of authorized vendors
- Acceptable Usage Policy shall be developed, distributed, and maintained for governing the acceptable usage of information assets and personal devices in FIVE's environment (**Refer:** FIVE Acceptable Usage Policy)

9. Access Control

The access control policy defines the objectives to ensure appropriate levels of access controls mapped to the identified assets are in place to protect the information in each application or system from unauthorized access, modification, disclosure, or destruction of information (**Refer**: FIVE Access Control Procedure)

- An access management procedure shall be developed, distributed, maintained, and followed to comply with the access management policy statements (**Refer**: FIVE Access Control Procedure)
- Users shall be granted access to information systems through a user access provisioning process based on approval from authorized personnel
- User access rights to information systems shall be revoked through a user de-provisioning process (**Refer**: FIVE Access Control Procedure: User Account Management)
- Password parameters as defined in the Identity and Access Management Procedure shall be configured and enforced for all users accessing information systems (**Refer**: FIVE Access Control Procedure: Privilege Management: Password Management)
- All user access including privileged and administrator level access to information systems shall be identified, documented, and maintained

- Privileged or administrator level access shall be restricted to authorized individuals based on the job responsibilities and business requirements
- Secure log-on procedures shall be enforced to access information systems
- Access rights and privileges granted to all users shall be reviewed by the respective Line Manager on a quarterly basis in accordance with the Identity and Access Management Procedure (**Refer**: FIVE Access Control Procedure: Privilege Management)
- Administrator and privileged accounts access activities shall be logged and reviewed on a monthly basis
- Information assets when accessed by external parties shall be logged, monitored, and reviewed on a monthly basis
- Solution shall be deployed for managing privileged access to information systems

9.1 Remote Access Management & Teleworking

The remote access management policy shall define the security requirements while connecting and accessing FIVE networks remotely

- A remote access management procedure shall be developed, distributed, maintained, and followed to comply with the remote access management policy statements (**Refer**: FIVE Access Control Procedure: Remote access standard
- Implement security measures to protect information processed or stored at a remote site
- FIVE shall implement preventive measures from the threat of unauthorized access to information or resources
- Multi-factor authentication and geo-restrictions shall be implemented, for all remote access connections to FIVE networks
- Remote access shall be granted only when using FIVE provided or authorized systems that are configured to meet the defined minimum-security requirements through an approval and authorization process
- Any teleworking equipment which provides remote access to the FIVE networks, and the authentication method that it uses to access FIVE resources, must be approved by the Group Director – IT & Group Director - Cybersecurity.
- Remote access connections shall be logged, monitored, and reviewed
- Access control mechanism and compliance check for remote access should be developed
- Training sessions shall be conducted for the users using mobile computing, to increase their awareness on the additional risks resulting from this way of working and the precaution that needs to be taken while using the device.

10. Cryptography

Cryptography is required to ensure that critical information assets are protected by the use of cryptography. Also, procedures exist for secure generation, storage, distribution, usage, change, revocation, destruction and archival of encryption keys. **(Refer**: FIVE Cryptography Procedure)

10.1 Use of cryptographic controls

- Users must be properly trained, and their systems must be configured by authorized personnel before they utilize encryption, digital signatures, or digital certificates for any FIVE business activity
- All IT devices (e.g., desktops, laptops etc.) must be encrypted. Encryption standards like AES, RSA, OpenPGP, etc. may be referred for the same
- The encryption needs of the data in motion will be determined by both the asset owner and asset custodian
- All data, which is Personally Identifiable Information (PII), as defined by the respective business jurisdiction and applicable laws (e.g., GDPR), shall be stored in an encrypted format
- All systems, for which the data is managed, stored, or otherwise used by another organization (for example, for cloud computing environments) outside FIVE, shall store all the relevant data in the appropriate encrypted format

10.2 Key management:

- The cryptographic keys shall be protected against unauthorized modification, substitution, unintended destruction, and loss.
- The secret keys associated with symmetric cryptographic algorithms shall be protected against unauthorized disclosure

11. Physical and environmental security

The purpose of this policy is to provide adequate protection to FIVE's information systems and facilities against unauthorized physical access and environmental threats. Appropriate controls shall be implemented to maintain the security of the information systems and equipment (**Refer:** FIVE Physical and Environmental Security Procedure)

- A physical access management procedure shall be developed, distributed, maintained, and followed to comply with the physical access management policy statements (**Refer:** FIVE Physical and Environmental Security Procedure)
- Access to FIVE offices, information processing and operational facilities shall be granted to authorized personnel based on the job description and business requirements
- Visitor entry into the IT rooms (e.g., server rooms) shall be restricted by appropriate security validations like checking the identity of the visitor, frisking of visitors, checking their belongings and bags, etc.
- All visitors carrying information processing equipment on the IT Server room (such as Laptops, Tablets, Smartphones) or media (such as CDs, Flash drives, and Hard disks), shall be asked to declare such assets and the same shall be recorded in a register at the security/ entrance gate
- Areas hosting information assets shall be protected against damage from fire, flood, earthquake, explosion, and other forms of natural or man-made disaster
- Physical access to Server rooms shall be pre-approved and recorded along with the date, time, and purpose of entry.

- Power and telecommunication cabling carrying data or supporting information services shall be protected from interference
- All equipment shall be maintained to ensure its continued availability and integrity. IT Team shall ensure that preventive maintenance for all IT devices is carried out at defined intervals for the continuous availability of these systems.
- Servers shall be protected from power failures or other disruptions caused by failures in supporting utilities
- The movement of equipment in and out of premises shall be monitored and requires authorization
- A clear desk policy for papers and removable storage media, and a clear screen policy for systems shall be adopted to reduce the risks of unauthorized access, loss of and damage to information

12. Operations Security

The Operations Security policy defines the controls that shall be implemented to prevent unauthorized access, misuse or failure of the information systems and processing facilities. FIVE shall ensure the effective and secure operation of its information systems and computing devices and define the appropriate controls to protect the information contained in and/ or processes by these information systems and computing devices (**Refer:** FIVE Operations Security Procedure)

12.1 Operation Management

- Operating procedures shall be developed and maintained for all processes to enable the system, network, and system administrators to perform their routine operations
- Monitor the performance, utilization, and availability of information processing resources to make future projections in accordance with Capacity Management process
- Segregation of duties shall be established to ensure that users do not have conflicting access to FIVE's information systems
- Development, test, and production facilities shall be logically separated to reduce the risks of unauthorized changes to the production system
- For instances where virtualization of FIVE systems is required, security configurations shall be implemented

12.2 Change Management

- All changes to information systems shall be applied in accordance with the Change Management process
- All change requests raised shall be identified, recorded, and assessed for information security risk and impact on FIVE's information systems
- Change requests initiated shall be submitted to the relevant stakeholders for review, approval, and prioritization of the proposed change

- A controlled acceptance test environment to build and test all changes prior to deployment shall be developed
- Implementation time window for the changes shall be determined and communicated to relevant stakeholders including users to avoid or minimize disruptions to the business
- A rollback plan to reverse the change (if unsuccessful) shall be defined and approved by all relevant stakeholders prior to the change
- Record of details of the changes shall be maintained
- Criteria for emergency changes and process to control the authorization and implementation of emergency changes shall be defined (**Refer:** FIVE Operations Procedure: Operational Change Management: Emergency Change)
- The change management process shall be integrated with other processes (e.g., Asset Management, Patch management etc.) to establish traceability, detect unauthorized changes, and identify change related incidents

12.3 Capacity Management

- Continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the business requirements of FIVE.

12.4 Configuration Management

- Security configuration baselines shall be defined and documented for all technology components based on security practices and standards
- Security configuration baselines shall be tested and approved, prior to implementing it in the production environment
- All changes to the security configuration baselines shall be logged and monitored
- Security configuration records shall be maintained to reflect changes in the status, version, location, associated problems, or changes to the configuration items
- Any deviations to the defined security configuration baselines standards shall be documented and compensating controls to be identified and implemented in accordance with the Information Security Policy Exception and Deviation Process
- Security configuration baselines shall be reviewed at least annually and updated based on changes in FIVE's technology components

12.5 Endpoint Security

- Centrally managed endpoint security solutions shall be deployed to protect endpoints as defined in the Endpoint Security Procedure (**Refer**: FIVE Endpoint Security Procedure: Endpoint Security)
- Endpoint security solutions shall be updated with the latest signature file when released by the OEM within 7 days

- The endpoint security solution shall be configured to perform background scanning.
- All FIVE systems shall be configured to prohibit usage of removable media devices such as USBs, and portable removable HDDs unless it is approved by the Head of Departments and Group Director of IT
- Detailed procedures shall exist to control the installation of software on operational systems (Refer: FIVE Hardening Procedures)

12.6 Monitoring and Log Management

- Systems shall be configured and enabled to log security events as defined in the Operations and Communication Security procedure
- Review of audit logs for user activities, exceptions, access, changes, and security events shall be centrally logged for all information systems, application, network devices, servers, and databases
- All configured logs shall be forwarded to a centralized SIEM system for aggregation and correlation
- Logging facilities and log information shall be protected against tampering and unauthorized access

13. Communications Security

The purpose of this section is to ensure that networks are managed and controlled to protect the information in the information processing facilities and maintain the security of information transferred within the organization and with external parties (**Refer:** FIVE Communications Security Procedure)

13.1 Network Security

- Network equipment and network paths shall be identified, documented, and updated at least quarterly and changes within the network environment
- A network architecture design based on the criticality of systems and security requirements shall be established and maintained
- The network architecture design shall take into consideration the principles of zoning, high availability, and operational resilience
- Networks shall be logically and physically segregated based on business requirements, sensitivity and criticality of the assets and information processed or stored on the systems
- Security measures shall be deployed based on the network architecture to secure the critical systems for IT
- Secure routing controls shall be implemented for networks to secure the network connections and information flows
- System clocks shall be synchronized using an NTP server that is connected to an accurate time source such as the Universal Coordinated Time (UTC)
- Implement a Network Access Control (NAC) solution for enforcing security policies and controlling devices/ user access to the network

- Network security monitoring shall be enabled by deploying network intrusion detection and prevention solutions

13.2 Electronic Messaging/ Email

- Information involved in electronic messaging/ emails shall be protected from unauthorized access, modification, or misuse of information
- Only official communications channels (e.g., MS Teams & Message Box) should be used for FIVE related official communications

13.3 Online Transactions and Public Information

- Online transactions shall be protected using encryption to prevent data leakage and unauthorized access to the data transmitted through such transactions
- Any information stored or generated by FIVE that is to be made publicly available shall be verified by PRO, and approved by the CFO/CEO before making it public

14. System acquisition, development, and maintenance

The purpose of this policy is to ensure that information security controls are identified and embedded during the system development, acquisition and requirements gathering phase of the project management. The systems developed or procured off-the-shelf are aligned with these requirements (**Refer:** FIVE Systems Acquisition Development and Maintenance Procedure)

- All new information systems and services that are acquired, developed, or enhanced shall undergo security risk assessments to ensure that appropriate security controls are identified and incorporated in them

14.1 Managing changes in Software Development

- All modifications to software shall be made in accordance with the Change Management process (**Refer:** FIVE System Acquisition Development and Maintenance Procedure: Program Control Procedures)
- Software developed by an external party shall have licensing agreements and contractual requirements or quality and accuracy of code

14.2 Deployment of information systems

- Applicable security hardening measures shall be applied on all systems prior to connecting to the production environment
- Secure testing like VAPT must be performed for web applications which are published on the Internet

15. Supplier relationships

The purpose of this policy is to establish a process for securing FIVE's information and/or information processing facilities that are accessed, processed, or managed by external parties (**Refer:** FIVE Supplier Relationship Procedure)

- Ensure that all services provided by external parties, are identified and the relationship is managed by nominated personnel
- Onboarding of any new products or services from the existing or new vendors/ suppliers shall be done only after information security risk assessment of such products or services is completed (**Refer:** FIVE Third-party Pre-Assessment Checklist)
- A contract shall be entered between FIVE and all external parties providing service to FIVE or using its information systems
- Contracts/ service agreements shall include information security requirements to ensure conformance to FIVE's information security policies and procedures
- The services to be provided by the external party shall be covered by a Service Level Agreement ('SLA') as defined in the Supplier Relationship Procedure (**Refer:** FIVE Supplier Relationship Procedure: Contract, Service Level Agreements and Non-Disclosure Agreements)
- Non-Disclosure Agreements (NDA) to protect FIVE's information assets shall be signed by external parties and by sub-contractors of the external party prior to sharing of any classified information
- Information security assessments of the vendor providing information services shall be conducted on a requirement basis

16. Information Security Incident Management

The purpose of information security incident management policy is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. (**Refer:** FIVE Information Security Incident Management Procedure)

- Information security incident response plan shall be defined and maintained to manage information security incidents
- Appropriate detection mechanisms shall be designed for timely detection of information security incidents.

- FIVE IT team shall ensure that in case of critical security incidents (**Refer:** FIVE Incident Management Procedure: Incident Classification and Escalation: Incident Severity), the management is notified, and appropriate action is taken
- Root cause analysis for critical reported incidents shall be carried out to identify the underlying cause and prevent recurrence.
- Security incidents that cannot be resolved immediately shall be escalated and if required, an effective and accurate workaround should be provided in case of any incident.
- All users shall be required to report any observed or suspected information security incidents to the IT Team/ Group Director - Cybersecurity
- Forensic analysis data and evidence shall be collected and retained
- A knowledge database with lessons learned reports shall be developed and maintained for information security incidents

17. Information security aspects of business continuity management

The Business Continuity Management policy provides the guidelines for inclusion of controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents and ensure that information required for business processes is readily & timely available. (**Refer:** FIVE Information Security Aspects of Business Continuity Management Procedure)
(**Refer:** FIVE IT BCM Policy)

18. Compliance

The purpose of compliance policy is to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and any security requirements. (**Refer:** FIVE Compliance Procedure)

- All relevant statutory, regulatory, and contractual requirements should be explicitly defined and documented for overall compliance (**Refer:** FIVE Compliance Checklist)
- The Security Steering Committee (SSC) should initiate an independent review of the Information Security policy
- The SSC should take corrective actions based on the findings of the review and the implementation should be carried out by the IT team
- Ensure compliance with intellectual property rights (IPR) requirements in terms of licenses of copyrighted software, legal terms & conditions, and or any other proprietary information used within the environment
- Information security controls including data privacy controls shall be implemented to comply with relevant legislation, regulations, and, when applicable, contractual clauses for FIVE entities

- Personal information related to users residing in FIVE's information systems shall be protected from unauthorized disclosure, loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements
- Information systems shall be reviewed on an annual basis for compliance with the organization's information security policies and standards. The findings of these reviews shall be reported to the SSC

19. Information Security Awareness and Training

The purpose of this policy is to establish and maintain an information security awareness and training program to ensure that users understand their information security responsibilities, information security policies, and adequately use and protect the assets entrusted to them. (**Refer:** FIVE Information Security Awareness and Training Procedure)

- Develop and implement an organization-wide information security awareness and training program for users having access to IT information assets
- New users joining the organization shall receive information security awareness training as part of their induction program
- The information security awareness and training program material shall be reviewed annually and updated as required to meet changes in FIVE's environment
- Effectiveness of security awareness and training program shall be measured in accordance with Information Security Awareness and Training Procedure
- Compliance with the information security awareness and training program shall be monitored and reported to the SSC on a quarterly basis
- Training records for all security awareness sessions conducted shall be documented and retained for a period of at least five years

20. Information Security Risk Management

The purpose of this policy is to ensure that information security risks that FIVE is or can be exposed to are identified, analyzed, recorded, mitigated, monitored, and managed by applying risk management principles. (**Refer:** FIVE Risk Management Procedure)

- Identify the scope for performing information security risk assessments
- Conduct periodic information security risk assessments to identify and evaluate information security risks, in accordance with Information Security Risk Management Procedure (**Refer:** FIVE Risk Management Procedure: Risk Assessment)

- Conduct an information security risk assessment before engaging with an IT supplier or vendor before obtaining any services or procurement.
- Risks shall be documented in a standard format to record, track, and manage risks
- Criteria to mitigate, avoid, transfer, or accept identified risks shall be in accordance with the Information Security Risk Management Procedure (**Refer:** FIVE Risk Management Procedure: Risk Mitigation and Treatment)
- Risk treatment plans to address the identified risks shall be identified, documented, assigned, and communicated to relevant stakeholders
- Any risks that cannot be mitigated to an acceptable risk level shall be approved by the SSC for risk acceptance (**Refer:** FIVE Risk Management Procedure: Risk Mitigation and Treatment)
- Cyber Insurance shall be availed as a risk mitigation method to transfer information security risks to a third party, especially where residual risk is greater than the risk acceptance level

21. Mobile Device Management

The purpose of the mobile device management policy is to define accepted practices and responsibilities for use of mobile devices which are authorized to connect to FIVE resources. (**Refer:** FIVE Mobile Device Management Procedure)

- A mobile device management procedure shall be developed, distributed, maintained, and followed
- Only those devices that are approved by FIVE IT shall be allowed to connect to the FIVE office networks
- Personal devices shall be prohibited to be connected to the FIVE office networks
- Information security controls shall be implemented to protect mobile devices as defined in Mobile Device Procedure (**Refer:** FIVE Mobile Device Management Procedure: Mobile Device Management)
- Mobile Device Management solution shall be used to control and enforce security requirements for mobile devices
- Maintain and update an inventory of all users registered with FIVE's mobile device management solution

22. Backup & Restoration

The purpose of the backup and restoration policy is to establish a routine process for taking backup copies of information and timely restoration of the backup. (**Refer:** FIVE Backup and Restoration Procedure)

- All applications, software, and data (including databases) essential for the continued operations of FIVE shall be identified, documented, and backed up
- Frequency of backup, type of backup and storage of backup shall be identified and documented based on the criticality of the information stored within the system
- Backups shall be retained in accordance with the requirements of FIVE and local regulatory laws (**Refer:** FIVE Backup and Restoration Procedure: Backup and Restoration: Storage of Backup Data)
- Backup data shall be always encrypted

- Backup data shall be provided for restoration only upon approval and authorization from Group Director – Cybersecurity
- Data restore logs shall be maintained
- Backup restoration process shall be tested and performed on an annual basis which will include restoration schedule, success criteria, test plan and test results and should be documented to verify the integrity and readability of backup media

23. Vulnerability and Patch Management

The purpose of this policy is to enable FIVE to proactively control risks through identification and remediation of vulnerabilities (**Refer:** FIVE Vulnerability and Patch Management Procedure)

23.1 Vulnerability Management

- Perform vulnerability scans using the latest signature file on all assets to identify, and evaluate information security vulnerabilities
- Prior to using automated scanners on FIVE systems, the impact of using such scanners shall be determined to ensure that they do not cause any disruption
- Vulnerability assessments shall be performed prior to the commissioning of a new system or applications
- Any evidence of compromise or exploited asset identified during vulnerability scans shall be reported to the SSC and Group Director – Cybersecurity
- All identified vulnerabilities shall be remediated based on the severity of the vulnerability and its impact to the respective systems
- In case of an application has been procured from a third-party vendor, VAPT report for the particular application from the vendor should be checked and reviewed

23.2 Patch Management

- All assets shall be patched to the latest patch level, prior to connecting them to the production environment
- Patches shall be assessed and evaluated for compatibility with systems, prior to being applied
- Deployment of the approved patches to the production environment shall be in accordance with the Change Management Procedure (**Refer:** FIVE Vulnerability and Patch Management Procedure: Patch Deployment)
- All applicable patches shall be tested by the IT team and approved by the Group Director - IT or Group Director - Cybersecurity before deployment to the production environment

24. Exceptions and Deviations

- All deviations from the information security policy shall be granted only based on business justifications and approvals from the Head of Department, Group Director – Cybersecurity and Group Director of Finance and Investments
- Deviation shall be granted for a specific cases and duration in accordance with the Information Security Policy Exemption process
- All requested deviations shall be subject to an information security risk assessment to identify the potential risks
- Remedial action shall be taken in response to deviation from approved policies and procedures

25. Appendix – Definitions and Abbreviations

25.1 Definitions

Terms	Definitions
Access Control	The process of granting or denying specific requests for obtaining and using information and related information processing services
Acquisition	Acquisition is a process defined by a series of phases that may include conceptualization, initiation, design, evaluation, development, testing, production, modification and disposal of services and systems
Anti-virus Software	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents
Application	Application arere an established set of task-oriented procedures designed to satisfy business needs.
Approve	Approve is an action which is performed by an authorized individual or function and has the final authority of acceptance and sign-off
Asset Custodian	Employees responsible for maintaining the information protection measures defined by the asset owner
Asset Owner	The term 'Information Asset owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of an information asset. The term 'Information Asset owner' does not mean that the person actually has any property rights to the asset. Routine tasks may be delegated, e.g., to a custodian looking after the asset on a daily basis, but the responsibility remains with the owner
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and

Terms	Definitions
	operational procedures, and to recommend necessary changes in controls, policies, or procedures
Audit Log	A security-relevant sequential record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, process, or event
Availability	The characteristic of information and supporting information systems being accessible and usable on a timely basis in the required manner.
Backup	A copy of files and programs made to facilitate recovery if necessary
Business Impact Analysis	BIA is a process used to determine the effect of an interruption of services on each business unit and the organization as a whole. The analysis can provide information on the short- and long-term effects of a disaster on such factors as loss of money, reputation and services provided
Business Continuity Plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption
Change Management	Change management is a formal process for directing and controlling alterations to the information processing environment. The objectives of change management are to reduce the risks posed by changes to the information processing, environment and improve the stability and reliability of the processing environment as changes are made. The change management process ensures that a change is: Requested Approved, Planned, Tested, Scheduled, Communicated, Implemented, Documented and Reviewed after the change
Classified information	Information assets or data that an entity claims as sensitive, secret, or confidential that requires protection of its confidentiality, integrity, or availability. Access to this information is restricted to people, process or other parties authorized by the company
Confidential	Confidential information is sensitive corporate information that, if exposed, can damage a company, either directly or indirectly. Information that is often considered confidential might consist of trade secrets, financial records, contracts and credit cards, strategies, customer lists, plans and pricing, salaries, and employment records, designs and prototypes and merger or acquisition plans.

Terms	Definitions
Confidentiality	The characteristic of information being disclosed only to authorized persons, entities, and processes at authorized times and in the authorized manner.
Control	Controls are safeguards or measures implemented to minimize security risks
Critical Information	The term "critical information" refers to information that can cause a loss or serious disruption in FIVE's ability to function if the availability of the information is denied or impaired. The criticality of information evaluates the data in terms of its effect on the company to perform its normal operations, management to make decisions, and competitive position. The criticality of information directly influences the frequency of its backup and offsite storage
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity
Data Classification	Grouping of company's entire information and business data into such categories, which denote criticality, sensitivity, and other attributes of information. Data classification aims at achieving four major attributes of information, viz. Confidentiality, integrity, availability, and reliability. Data classification scheme will also influence the nature, type, and extent of information security solutions to be deployed in the company.
Data Owner	Data ownership is the act of having authorized rights and complete control over a single piece or set of data elements. Also referred to as 'Information Asset Owner'
Disaster Recovery Plan (DRP)	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Entity	An entity refers to the FIVE Hotel & Resorts locations the defined policy and procedures are applicable to
Incident	An Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information or Information Systems. It is related to exceptional situations or a situation that warrants intervention of senior management, which has the potential to cause injury or significant property damage

Terms	Definitions
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's IT systems(s)
Information	Applies to any storage, communication, or receipt of knowledge, such as fact, data, opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.
Information Asset	Any information or asset that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) and Operational Technology (OT) system, network, circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), documents, records, reports, SOPs, and related hardware (e.g., locks, cabinets, keyboards)
Information Processing	Information processing entails any activity on the information including, but not limited to, creation, modification, deletion, storage, transmission, replication, encryption, decryption, etc.
Information Processing Facility	An information processing facility is defined as any system, service, or infrastructure, or any physical location that houses these things. A facility can be either an activity or a place; it can be either tangible or intangible
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide Confidentiality, Integrity and Availability
Information Security Awareness and Training	Activities which seek to focus an individual's attention on an (information security) issue or set of issues
Information System	Any computerized system used for managing and processing any company related information within a single entity or crossing multiple entities
Information Technology (IT)	Information Technology refers to development, maintenance, and use of computer software, systems and networks that is used in the acquisition, storage, manipulation, management, transmission of information throughout and between organizations. For e.g., ERP, mail systems, Point of Sales (POS) systems, payroll systems, etc.
Information User	Personnel granted access to information assets by the data owner

Terms	Definitions
Integrity	The characteristic of information being in its intended state of accuracy and complete, and the information systems' preservation of that state and completeness.
Intellectual Property Rights	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Mobile Device	A mobile device refers to the trend of employees using personally, or company owned devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data. Devices could include smartphones, tablets, handheld devices, or USB drives
Multi Factor Authentication	Multi Factor Authentication is an electronic authentication method in which user authentication process uses two or more factors to grant access to an information systems or application, typically: 'something you have' and 'something you know'
Online Transaction	Companies' software, data, and other information being made available or allowed to be accessed using a publicly available system, typically using internet
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization
Physical access controls	Physical access controls monitor and control the environment of the workplace and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls
Policy	A policy is a broad statement of principle that presents management positions for each defined control objective(s). Policies are intended to be long-term and guide the development of rules to address specific situations. Policies are interpreted by standards, guidelines, and detail procedures

Terms	Definitions
Policy owner	Person or group of persons, who is responsible for envisaging, designing, finalizing, and mandating various types of policy decisions in the company. Policy owner may appoint appropriate number of executive owners for respective policies.
Processes	Processes is definite way of doing things, a series of steps to an end or a set of established forms and methods for conducting legal and business affairs. The process always delineates from policies and substantiate ways and means of implementing policies. Within a company, process refer to specific platforms and applications, and outline steps, which must be taken within the company when implementing security. They follow corporate policy and procedures as closely as possible, while adhering to specific technical or procedural requirements within the company.
Patches	A patch is a set of changes to a computer program, or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bugfixes or bug fixes
Privacy	Restricting access to subscriber or Relying Party information in accordance with applicable law
Resource	Resources can be any skilled personnel, process, tools, or asset which will support an activity or initiative
Remote Access	Functionality within computer systems and in particular an operating system, to enable the user to connect local computer with a remotely stationed systems or set of systems
Residual Risk	The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat
Risk Acceptance	It is the decision to accept a risk
Risk	Risk is the quantifiable likelihood of potential harm that may arise from a future event
Risk Assessment	The overall process of Risk Analysis and Risk Evaluation
Risk Management	The coordinated activities to direct and control an organization with regard to risk
Risk Treatment	The treatment process of selection and implementation of measures to modify risk

Terms	Definitions
Recovery Time Objective (RTO)	The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs
Recovery Point Objective (RPO)	Recovery point objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization.
Security Event	A security event is a change in the everyday operations of a network or information technology service indicating that a security policy may have been violated or a security safeguard may have failed
Security Incident	A Security Incident is a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. However, adverse events such as natural disaster, hardware/software breakdown, communication link failure, power disruption, etc. are outside the scope of this Plan and should be addressed by the System Maintenance, Disaster Recovery Plan and Business Continuity Plan
Segregation of Duties	Segregation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users
System	An umbrella term for the hardware, software, physical, administrative, and organizational issues that need to be considered when addressing the protection of a company's information resources.
Organization	An organization is group of companies, people with a defined and common objective, goal, and purpose such as business or department
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service
User	User refers to all employees, third-party service providers, and contractor employees accessing FIVE resources, office/corporate network, systems, and information

Terms	Definitions
Version	A change effected in computer systems/ systems environment by replacing the existing system by implementing new set of programs of the same system to enhance and upgrade the system capabilities and functionality
Virus	A virus is an unauthorized and malicious program which replicates itself and spreads onto various data storage media such as magnetic disk, tapes and across the network. Viruses threaten the integrity and availability of data.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

25.2 Abbreviations

Terms	Descriptions
ISC	Information Security Coordinators
CIA	Confidentiality, Integrity, Availability
DR	Disaster Recovery
DRP	Disaster Recovery Plan
BCP	Business Continuity Plan
FIVE	FIVE Holdings (BIV) Limited
ID	Identity
IPR	Intellectual Property Rights
ISMS	Information Security Management System
SSC	Security Steering Committee
IT	Information Technology
KPI	Key Performance Indicator
NAC	Network Access Control
NDA	Non-Disclosure Agreement
OEM	Original Equipment Manufacturer
RPO	Recovery Process Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SOPs	Standard Operating Procedures
USB	Universal Serial Bus