Take5people
NOW YOU CAN

Information Security Policy

Jan Rautiainen

4/1/2020

Document Control

Document Owner	Classification	Version
Jan Rautiainen	PUBLIC	1.2

Revision history

Version	Changed by	Date	Change detail
1.0	Jan Rautiainen	1/4/2020	Initial version.
1.1	Jan Rautiainen	28/12/2020	Update the location URL.
1.2	Jan Rautiainen	26/8/2021	Add Password Policy and update public link.

Review history

Version	Reviewed by	Date	Conclusion
1.0	Steve Collins	3/4/2020	Review passed.
1.1	Steve Collins	28/12/2020	Review passed.
1.2	Steve Collins	27/8/2021	Review passed.

Approval history

Version	Approved by	Date	Approved (Yes/No)
1.0	Steve Collins	3/4/2020	Yes
1.1	Steve Collins	28/12/2020	Yes
1.2	Steve Collins	27/8/2021	Yes

Distribution

Copy	Issued to	Location
Master	Public	https://take5people.com/wp-content/uploads/Take5People-Information-Security-Policy-EN-v1.2.pdf

Contents

Introduction

The continuity of the Take5 People regionally (“T5P”) is highly dependent upon the way which the information resources are managed. The principles used in setting the foundations for the policies governing information security management are:

- Information resources that support information processing are important assets (“information assets”) which must be appropriately protected from accidental or intentional compromise.
- The confidentiality, integrity and availability of information assets are essential for ensuring legal compliance and for maintaining competitive edge and the image of T5P.
- Information assets are provided to support business processes and should be used to derive benefit for T5P.
- All personnel who use information assets have a responsibility to protect them, and to minimize the risks that might result from inappropriate use.

Throughout the document the terms MUST, SHALL and SHOULD are used carefully. “Musts” and “shalls” are mandatory and not negotiable; “shoulds” are goals for T5P. The terms “data”, “information” and “information asset” are used interchangeably in the documents.

Hierarchy of Information Security Policies and Standards

The set of Information Security Policies and Standards consists of documents with different levels of details:

- **Policies**

  Policies are high-level statements driven by T5P's requirements. They are technology and process independent statements setting the general principles, goals and objectives for T5P. They are not statements of how the goals and objectives will be accomplished.

- **Standards**

  Standards are the next level in the hierarchy with increasing levels of detail for business requirements.

  Standards still remain platform independent. They are directed to the implementation of policies for specific subject areas. Standards can be further broken down into two types, with varying levels in their implementation.

  - **Requirements** are activities that must be followed – there is no leeway within a requirement.
  - **Guidelines** are not as stringent as requirements – guidelines should be followed, unless there is a compelling business reason for not doing so (for example, if there are specific legal requirements within a jurisdiction prohibiting the implementation of such a requirement, then there is a compelling business justification for not implementing the standard.)

- **Procedures**

  Procedures are process-level and/or platform-specific instructions for implementing Policies and Standards. One standard may require multiple procedures – one for each platform to satisfy the standard. For example, a standard dealing with password length would require procedures at least one separated for each platform – Windows, MacOS, Linux, etc. – where that standard is implemented.

Objective

The objective of this "Information Security Policies" document is to outline the principles to which all users of information assets in any form owned by or entrusted to T5P shall handle such information asset. The principles cover the following areas:

Defining the confidentiality, integrity and availability requirements for data and information resources used to support the T5P's objectives.

Ensuring that the security requirements of those data and information resources are effectively communicated to all individuals who come in contact with such information.

Using, managing and distributing those data and information resources in any form (electronic or physical) in a manner that is consistent with their confidentiality, integrity and availability requirements at all times.

Definition of Information Security

Information security is the collection of critical methods to protect information and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction and it is applicable to the lifecycle of the information from creation, use, transfer and storage to disposal.

Information security is primarily concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: digital (e.g. data files), material (e.g. printed papers), or unrepresented information (e.g. knowledge of internal affairs). These include text, picture, audio and video and covers information transmitted by mail, email, oral communication, telephone etc.

T5P requires appropriate control measures for all forms of information to ensure their confidentiality, integrity and availability and avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

- **Confidentiality** means protecting information from unauthorized access or disclosure
- **Integrity** means protecting information from unauthorized or improper modification and destruction
- **Availability** means to ensuring timely and reliable access to and use of data and information resources.

T5P shall also adopt control measures to ensure the authenticity, accountability, non-repudiation, and reliability of information and information services depending on circumstances.

- **Authenticity** means assuring the correctness of the claimed identity of an entity.
- **Accountability** means assuring the traceability and responsibility of an entity for its actions and decisions.
- **Non-repudiation** meant preventing the future false denial of involvement by any entities.
- **Reliability** means assuring the correctness of service, and behavior and result of service is consistent and predictable.

Scope

This document is used as the T5P-wide Information Security Policies and all activities performed relating to the information resources must comply with the policies unless a written approval was obtained from the Senior Management Team, which is the approval body of this standard. Also, this policy must be published and communicated to all T5P's employees and relevant external parties.

Purpose

The purpose of these policies and standards is to ensure that due care is exercised in protecting T5P's information assets. Due care is defined as the economical and practical protection of information at a level commensurate with its value to T5P and its Customers. The value of the information is determined by considering not only the cost of its development, but also its non-monetary value, including intangible worth (e.g. intellectual property and competitive value) and rights of personnel affected (e.g. privacy). The value of information can also be impacted by its misuse. Good Information security can facilitate cost avoidance through the prevention of misuse.

Annual Review

The Information Security Officer ("ISO") in the Technical Team is responsible for the reviews and updates of this document from time-to-time to keep up with any changes in this policy and request approval from Senior Management Team should changes be made.

Terms and Definitions

For the purpose of this set of documents, the following terms will be used:

Asset owner

Asset owner is the person or group of people identified by management as having responsibility for the maintenance of the security of that asset. The asset owner may change during the lifecycle of the asset.

- The owner does not normally or necessarily personally own the asset. In most cases the employing organization, its customers or suppliers will be the entity with property rights to the asset. This includes but is not limited to, Customers' master data documents.
- The term asset owner is used in this document to refer to the current entity withholding the Information, that is considered to be one type of asset.

Asset

Asset is anything that has value to the T5P and its Customers. There are many types of assets, including:

- information;
- software, such as a computer program;
- physical, such as computer;
- services;
- people, and their qualifications, skills, and experience; and
- intangibles, such as reputation and image.

IT asset

IT asset is the asset that related to the processing of digital information. Types of IT asset include hardware, software, digital storage media, IT services, etc.

Information asset

Information asset is one type of asset and IT asset. Information assets are knowledge or data that has value to the T5P or its Customers regardless of form or format.

Information resources

All data, information as well as the hardware, software, personnel and processes involved with the storage, processing and output of such information. This includes data networks, servers, PC's, storage media, printers, photo copiers, fax machines, supporting equipment, and back-up media.

Information Security Policies

1. Organization of Information Security

Each member of the T5P, including staff members and other possible third party entities, that are contractually engaged with the T5P are responsible for the security and protection of information resources over which he or she has control. He or she is obliged to adhere to the T5P's information security policies, standards, guidelines and procedures, and protect information resources from unauthorized intrusions, malicious misuse, or inadvertent compromise; and to preserve physical and logical integrity of these information resources.

The following bodies in T5P are responsible for the governance of the Information Security in the T5P:

"**Information Security Officer**" (ISO). This is the top-most authority in the Information governance structure of T5P. It represents the management of T5P and is responsible for endorsing the policies, guidelines, rules and regulations governing the IT provision in T5P. It is also responsible for making recommendations on resource and budget allocations to the IT-related initiatives to T5P and the monitoring and reviewing of the implementation of IT initiatives.

"**Senior Management Team**" (SMT). It is the body for reviewing, and collecting the opinions on this T5P's Information Security Policies and Standards ("ISPS"), SMT consists of members from key Senior Management Team of T5P.

"IT/Technical Team". It contains the members of T5P Technical Team. The Technical Team, while maintaining the T5P-wide ISPS, is also responsible for meeting the requirements in this ISPS.

- The ISO is responsible for the strategic development and co-ordination of all information services and technology in T5P. It is also responsible for all security related activities. Annual review of T5P-wide ISPS implementation is also its responsibility, recommending changes and enhancements to this ISPS and proposing those changes to be approved by SMT.
- The SMT is responsible of reviewing and evaluating this ISPS and approving it as a whole.
- The IT/Technical Team is responsible for the provision of central computing facilities and technical services including rendering to computer and network in the T5P. It is responsible for implementing and managing T5P's central information systems. It works in partnership with different departments to integrate information technology into administrative processes.

"Departments" and "Departmental Information Technology Support Units" (Departmental ITSU). The Departments use the T5P's information in their daily operations. Some of the Departments maintain their own departmental IT functions and operations. Their staff members operations must meet the specific departmental needs. Head of departments or their delegates shall ensure the conformity of their use of information and information resources to T5P-wide ISPS.

"System Owner". System Owner is an individual or an entity, which is responsible for the overall procurement, production, development, modification, maintenance, use of that particular system.

While the System Owner has final responsibility for proper operation of the system, the System Owner could delegate some of the operational tasks to IT/Technical Team.

2. Information & IT Asset Inventory and Ownership

An inventory list of important assets associated with information resources must be properly documented and maintained for record-keeping and auditing purposes.

The establishment of roles, responsibilities and accountabilities are needed for proper management and protection of T5P's information assets.

All information and IT assets obtained by T5P, used for work-related purpose, or storing the T5P's or Customers' Information are subject to the T5P's control. They can only be disposed in accordance with the requirement defined in Section "**4) Information Classification and Handling**" policy of this document.

3. Acceptable Usage

T5P values academic and intellectual freedom and encourages the use of T5P's information resources to support T5P's affairs and its mission of education, service and research. Priority must be given to the use of the information resources for the official affairs of T5P.

T5P recognizes the trend of "Bring Your Own Device" (BYOD). Regardless of the ownership, "Information resources" means all information and communications technology; hardware and software; data and associated methodologies; infrastructure and devices that are:

- controlled or operated by T5P;
- connected to the T5P's network;
- used at or for the T5P's activities;
- brought onto the T5P's premises.

Information resources include but not limited to:

- Computers and mobile devices – such as desktops, laptops, tablets, Smart phones, Personal Digital Assistances ("PDAs");
- Computer systems – such as the T5P's information systems and applications;
- Storage devices – such as Universal Serial Bus ("USB") flash memory devices, Compact Discs ("CDs"), Digital Versatile Discs ("DVDs"), floppy disks, network multi-function printers with built-in memory for caching printouts or storing scanned images;
- Telecommunication equipment – such as switches, routers, Private Branch Exchange ("PBX") systems and phones, VoIP systems and phones;
- Networks – such as Intranet and Internet via wired or wireless connections;
- Software, databases and any other similar technologies as they come into use; and
- Information or data stored in any carriers, service providers and third parties, such as Google Docs or DropBox and other such third party cloud storage services.

The use of information resources, including their handling and storage, must be legal and must be of the highest ethical standards, and must not involve with activities and/or material(s) unacceptable to T5P's environment which include, but not limited to acts of a malicious or nuisance nature, invasion of privacy, violation of copyright and licensing, harassment, bullying, hacking, altering the settings on any information resources without authorization, plagiarism, impersonation/identity theft or spoofing

4. Information Classification and Handling

T5P must classify all its information into appropriate levels (e.g. restricted, confidential, internal and public) to indicate the need, priority and degree of protection required.

The following classification levels shall be used for classifying the T5P's information assets:

- **RESTRICTED**. This classification applies to sensitive information that is strictly restricted by T5P, the government or any other agreements between T5P and third parties (including the government).

  Throughout the scope of this set of Information Security Policies and Standards, the terms "**RESTRICTED**" and "**SECRET**" are used interchangeably.

- **CONFIDENTIAL**. This classification applies to sensitive information that is intended for use by authorized personnel within the T5P.

- **INTERNAL**. This classification applies to information that is intended for internal use within a department or T5P.

- **PUBLIC**. This classification applies to information that has been approved by authorized parties within the T5P for Public Consumption.

Every member of T5P has responsibilities to consider security during the entire life-cycle of information in the course of their works.

T5P has defined retention periods for certain kinds of information. Each member of T5P shall observe these requirements. Section "16.2) **T5P Policies and Regulations**" of this document listed some sources of the T5P's Policies.

Each T5P Department should establish procedures appropriate to the information held and processed by it, and ensure that all staff members are aware of those procedures.

5. Human Resources Security

5.1. Prior to Employment / Engagement

T5P's staff members and possible third party members must understand their responsibilities and must be suitable for the roles they are considered for in handling or use of information assets. T5P must implement appropriate controls to reduce the risk of theft, fraud or misuse of the T5P's information assets and resources.

- **Roles and responsibilities**. All the T5P's staff members and possible third party users are obliged to follow the security roles and responsibilities defined and documented by the T5P, and their respective T5P Departments.
- **Screening**. Pre-employment screening is a mandatory requirement for candidates whose roles or positions may have access to sensitive information.
- **Undertaking**. All T5P's staff members must agree to and sign a Confidentiality Pledge to indicate that they fully understand their responsibilities with respect to information security, and agree to comply with the T5P's ISPS.

5.2. During Employment / Engagement

The T5P's staff members and possible third party users shall be aware of information security threats and concerns; and of their responsibilities and liabilities; and are expected to be properly equipped to support the T5P ISPS in the course of their normal work activities and to reduce the risk of human error.

- **Management responsibilities**. T5P's management is responsible for ensuring that all the T5P's staff members and possible third party members shall comply with the T5P's ISPS.
- **Information security awareness, education and training**. All the T5P's staff members and possible third party users should receive appropriate information security awareness training and regular updates of the T5P's ISPS relevant to their job functions.
- **Disciplinary process**. All the T5P's staff members and possible third party members who have committed a security breach are subject to T5P's disciplinary actions.

5.3. Terminations or Change of Employment / Engagement

The T5P's staff members and possible third party users shall exit or change employment / engagement relationship with the T5P in an orderly manner.

- **Return of assets**. All the T5P's staff members and possible third parties must return all of T5P's assets in their possession in condition acceptable to T5P upon termination of employment and contractual relationships.

- **Removal of access rights**. Access rights to information and/or information resources must be removed or de-activated upon termination of the responsibility, employment and contractual relationships.

- **Change of responsibility or employment**. T5P shall manage change of responsibility or employment as well as the termination of employment or responsibility. The new responsibility or employment should be managed as described in Section 5.1.

6. Physical Access Security

The equipment, records, and data comprising IT operations represent a critical asset for T5P and they must be protected adequately commensurate with their value, confidentiality, and criticality of the information or data stored or accessible and the identified risks. Physical access control over T5P's information resources must be implemented and should include the following implementation elements:

- Equipment control (into and out of office) if applicable;
- A facility (e.g. place, site, office and room) security plan;
- Physical entry control including an evacuation plan and information asset protection plan, as appropriate, during an emergency evacuation;
- Procedures for verifying access authorizations prior to physical access;
- Maintenance records, including but not limited to, records of infrastructure changes such as adding or deleting network segments, adding servers, etc.;
- Need-to-know procedures for personnel physical access;
- Sign-in for visitors (e.g. staff members, contractors, customers or prospects) and escort, if appropriate; and
- Testing and revision of the physical access controls if applicable.

These apply to all information processing facilities and premises, including local data center, general offices and premises of contractors performing service for the T5P.

7. Environmental Security

Environmental security is important for the T5P to ensure its investment is capable of meeting its performance and uptime objectives. T5P's premises should be protected physically against damage from fire, flood, wind, earthquake, explosion, civil unrest, theft, robbery, vandalism, and other forms of natural and man-made risk.

Environmental monitoring of the following conditions must be carried out for all business critical systems and are strongly recommended for all other hosts and server systems when applicable:

- Air conditioning (temperature and humidity);
- Fire and smoke detection and control;
- Electrical power supply;
- Uninterrupted Power Supply ("UPS") installations;
- Water leakage;
- Alarm and emergency systems; and
- Exterior, interior, grounding and other structural protection.

The relevant departments, controllers or custodians are responsible for ensuring that these conditions are complied with.

8. Communications and Operating Management

T5P must ensure that the operational procedures for correct and secure handling of information resources are documented and made available to appropriate staff members and possible contractors. The level of detail should match the criticality of the information being processed and complexity of the operations concerned.

T5P shall segregate the duties and areas of responsibility of staff members and possible contractors to reduce the risk of unauthorized or unintentional access, modification or misuse of information assets. The level of segregation should match the confidentiality and security requirements of the information being processed.

9. Change Management

T5P must ensure changes to its information systems, telecommunication equipment, software, and other information resources will not result in adverse impact on the confidentiality, integrity and availability of the T5P's IT environment unless a written approval on exemption being granted was obtained from the Senior Management Team (SMT). All changes must be documented, authorized and in line with the T5P's operational and security requirements. In particular, the following items should be recorded:

- Change Request, with initiator, approval, implementer, and reviewer records
- Planning and testing of changes
- Assessment of potential impacts, including security impacts
- Fallback procedures

T5P should ensure that personnel responsible for change development and production migration are properly segregated. When duties cannot be separated, compensating controls should be implemented, for instance, a supervisory level employee should review the system regularly and/or after change.

T5P should assign dedicated resources to monitor the change processes. Periodic system migration log checking of production systems should be performed by personnel with sufficient technical knowledge and independent from the change promotion teams responsible for the systems.

10. Network and Platform Security

10.1. Network Segregation

T5P shall properly protect all networks with appropriate security measures and appropriate equipment. Network addresses, network configurations and related systems or network information shall be properly maintained and shall only be released to authorized parties.

T5P shall segregate the office networks into separated network environments according to the usage, classification of information and services hosted in the network:

- **"Untrusted Network".** Devices on the untrusted network are either accessible to all the members of T5P, or fully controlled and managed by the general users or owners of the devices (e.g. tablets of individuals).

  Since these devices may be abused, or may not be properly configured, untrusted networks shall be used to isolate these devices. Direct access to any of the sensitive information or servers is not allowed.

- **"Managed Network"**. Devices on the managed network are managed by Departmental ITSU, IT/Technical Team and/or users of the devices. Access controls are enforced on these devices, which are accessible to named users or shared by small group of named users (e.g. office desktops for staff members). Managed network shall be used for day-to-day office tasks and activities of T5P Departments.

- **"Secured Network"**. Critical services shall be hosted in secured network, and only be accessible to authorized staff, appropriate possible contractors and third party members. "RESTRICTED" and "CONFIDENTIAL" information shall primarily be stored in secured network, and only be transmitted to devices on other networks for processing when needed. Appropriate security controls shall be implemented to protect devices, services and information in the network.

T5P shall maintain multiple secured networks to segregate services and applications of different natures or security requirements.

- **"(Departmental) Internal network".** Departmental Internal networks are sub-networks inside the T5P network. They are controlled and maintained individually by the respective T5P Departments or trusted staff members. When "RESTRICTED", "CONFIDENTIAL" and "INTERNAL" information are required to be hosted and/or processed, departmental networks must be segregated into the "untrusted network", "managed network" and "secured network". The security levels of these departmental internal networks must conform to T5P's ISPS.

T5P shall manage and control the networks to maintain network security. Staff members and possible contractors and third party members shall not connect unauthorized devices into the networks or by any means to lower the security levels of the T5P's networks. Connections between

networks must not compromise or downgrade the security of information processed in the networks.

T5P shall document, monitor and control wireless networks with connection to its network. Staff members and possible contractors and third party members are prohibited from connecting unauthorized wired/wireless network devices and/or setting up peer-to-peer or ad-hoc wireless network with connection to T5P's networks, and sharing T5P's networks to uncontrolled devices.

Proper authentication and encryption security controls shall be employed to protect data communication over wired/wireless networks with connection to T5P's networks.

10.2. Internet and External Network Security

Centrally arranged Internet gateways are managed by IT/Technical Team when applicable. T5P Departments may arrange and manage their own Internet gateways according to T5P's prevailing policy and regulation.

All gateways (including Internet gateways and gateways to External Networks between T5P, partners of T5P and/or the remote sites of T5P) must be approved by and registered with IT/Technical Team, and all Internet access shall be channeled through registered gateways. All gateways must also conform to the "Network and Platform Security Standard" of T5P.

All Inbound and outbound traffic to and from the T5P's networks and systems must pass though the registered gateways.

"**RESTRICTED**", "**CONFIDENTIAL**" and "**INTERNAL**" data must be encrypted when transmitted over an untrusted network.

In circumstances where it is not feasible to fulfill the standards or the network is designed to meet special purposes, the IT/Technical Team shall isolate the network from the other networks of the T5P. The owner shall register the network with IT/Technical Team; shall implement appropriate security control and must not connect this network to the other systems of T5P.

10.3. Application, Service and Platform Security

The owners, controllers or custodians of Information Systems must ensure that their Information Systems are protected from threats and must implement the following:

- Anti-virus and Firewall Systems
- Intrusion detection Systems if feasible
- Information and System backup Systems
- Network and Application logging and monitoring Systems
- Application and Platform Configuration Management and Hardening
- Hardware and Software Patch Management
- Configuration management

11. Access control

Access control to critical, important information assets based on functional and security requirements of T5P is essential to safeguard the confidentiality, integrity and availability of information assets within T5P.

11.1. Access Control Policy

T5P must implement the following:

- Access control that will restrict access to resources and allow access only by privileged entities. Either of the following implementation features may be used:
    - Role-based access; and/or
    - User-based access;
- Security event control that will record and examine system activities, especially those performed by privileged accounts, and respond to “security events”;
- Authorization control that will require obtaining consent for the use and disclosure of T5P’s information; and
- Password control that corroborate an entity – the individual user of a data network or system, or a computational process – to whom it claims to be.

T5P Departments shall regularly review access privileges to services and data granted to roles and users; to ensure the appropriateness of privileges possessed by the relevant roles and individuals.

11.2. Password and Screen Lockout Policy

All accounts of T5P’s information systems must be password protected to help maintain the confidentiality, integrity and availability of T5P’s data as well as to help protect T5P’s information resources.

Each member of T5P is responsible for ensuring that strong passwords are used and the passwords are maintained according to T5P’s password standard. This is to reduce overall risks to T5P by helping authorized users reasonably avoid security and privacy risks that result from weak password choices.

T5P shall also enforce screen lockout policy on user desktops and laptops of all staff members except desktops designated or special purpose, e.g. monitoring console for network performance.

12. Information System Acquisition, Development and Maintenance

T5P must ensure that information security is considered throughout the lifecycle of any system that holds and processes T5P's information assets, from conception and design, through creation and maintenance, to ultimate disposal. This policy outlines the basic requirements and responsibilities to achieve this.

12.1. Security Requirement of Information Systems

Any department with requirements for IT systems must discuss them with IT/Technical Team at the project initiation stage.

Business requirement documentation for new systems or enhancements to existing systems must contain the requirements for security controls. Security vulnerabilities must be recognized from the outset through undertaking a risk assessment and the security requirements must be developed alongside the functional requirements.

Appropriate controls and audit trails must be designed into applications to prevent error, loss and unauthorized modification or misuse of information in application systems.

Application systems must implement input validation to ensure that data input is properly encoded and sanitized (i.e. filter all unaccepted and unsupported input, reject insertion and injection of codes, commands and instructions, eliminate buffer overflow and divided by zero, prevent path transversal, etc.). Input validation must be mandatory at server-side and client-side as appropriate.

12.2. Security in Development and Implementation

T5P must ensure an IT system is comprehensively tested for all its functional and security features prior to the implementation in the production environment.

Any of T5P's data that is used during the development and test phase of preparing application software must be protected and controlled.

Security controls must be applied to the implementation of IT systems in the production environment.

Application must be tested for an extensive period against predetermined criteria and methodologies by personnel not directly involved in the development of the system.

Testing results must be documented and retained. Testing results must be accepted and approved by system owner before the application rollouts.

13. Password Policy

All Take5 staff passwords must be

- Minimum 8 characters long
- Contain at least
    - One small letter
    - One capital letter
    - One number
    - One special character
- Must not contain
    - User name
    - User birthdate
    - User phone number
    - User national id or part of it
    - User passport number
    - User driver license number
    - A word “password”

14. Information Security Incident Management

As a key part of any organization’s overall information security strategy, it is essential to have in place a structured well planned information security incident management approach.

14.1. Responsibility

IT/Technical Team will manage all information security incidents with the assistance from all parties within T5P, this include but not limited to the Senior Management Team, Department heads, Research & Development and operational staff.

An Information Security Incident Response Team (“ISIRT”) shall be established and led by ISO to provide T5P with appropriate personnel for assessing, responding to and learning from information security incidents, and providing the necessary co-ordination, management, feedback and communication.

All staff members of T5P have responsibilities to report any security incidents to IT/Technical Team or ISIRT.

Security incidents include but not limited to:

- Known information security breaches, such as theft;
- Disruptions or loss caused by the failure of a security mechanism, such as computer virus infection or abnormal system behavior; and
- Known or suspected security incidents, such as system outage or traffic congestion due to a hacking attempt (i.e. intrusion or DDOS).

14.2. Information Security Incident Reporting and Response Procedure

T5P's staff members and possible contractors and third-party users who come across any evidence of information being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy information must report such information to his or her immediate supervisor, to T5P IT/Technical Team or ISIRT. "Critical" or "Significant" security incidents should not be investigated by individuals without the authorization of the ISO.

An Information Security Incident Reporting Procedure must be defined to handle information security incidents. The procedure will include the following:

Types and severities of information security incidents;

- Incident reporting procedures setting out the actions and point of contact;
- Incident response procedures for different types and severities of incident, including appropriate analysis and identification of causes, containment, communication with those actually or potentially affected by the incident, reporting of the incident to appropriate authorities, planning and implementation of corrective action to prevent reoccurrence as appropriate;
- Seizure of IT equipment and the relevant data and log files, collection and use of audit trails and similar evidence as part of the incident management and investigation process, and appropriate management of this evidence for use in subsequent legal or disciplinary proceedings;
- Formal controls for recovery and remediation, including appropriate documentation of actions taken; and
- Mechanisms used to perform ongoing monitoring of information resources to detect events and incidents.

14.3. Post Information Security Incident Review Procedures

After information security incidents have been resolved or closed, the following review activities are necessary:

- Identifying the lessons learned from information security incidents; and
- Identifying improvements to information security safeguard implementation, as a result of the lessons learned, whether from one information security incident or many.

14.4. Information Security Awareness Training

Heads and supervisors of the T5P Departments should ensure that appropriate information security awareness training is regularly conducted for their staff members.

The training programs should:

- Include reviewing T5P's information security policy, guidelines, procedures, and standards, as well as departmental procedures and best practices established to safeguard sensitive information;
- Conform with the laws governing specific categories of confidential information, such as the Personal Data (Privacy) Ordinance, etc.;
- Include topics such as password management, best practices for protecting confidential information, incident reporting, and security reminders regarding current threats and recent incidents to technical environments in which individuals are working; and
- Include awareness on the part of all T5P staff members, and possible contractors and third-party members in timely reporting information security incidents.

15. Business Continuity Management

Business Continuity Plans ("BCP") and Disaster Recovery Plans are required to maintain the operations of T5P in the event of an incident or a disaster.

Each regional office must develop plans that will allow it to perform its core required operations in an alternative fashion as well as an appropriate disaster recovery policy and plans for their working environment.

Each information system of T5P must have periodic backups of data, facilities for continuing critical operations available in case of an emergency, and disaster recovery plans in place. While the development of a BCP is a general business issue with the IT component as a part of the overall plan, having a BCP is a significant element in providing the "availability" component of T5P's Information Security.

An effective business continuity management must include the following:

- A Crisis Management Team, which is an administrative and decision-making group of Senior Management Team that is responsible for coordination of BCP in the event of an incident or a disaster;
- An emergency operation centre and operational plan, if applicable;
- A disaster recovery and business resumption plan; and
- Regular testing and revisions procedures.

16. Information System Internal Security Assessment

Internal Security Team of T5P conducts Independent Internal Security Audits in T5P. The roles and responsibilities of Security Team are defined by the Internal Security Audit Charter of T5P.

T5P must ensure that all information systems and applications, which are critical to T5P's operations or contain sensitive information of T5P, and its related infrastructure, shall be evaluated as an ongoing process to improve the quality of its operations. This policy shall apply to all the Departments of T5P.

Periodic information system internal assessment should be performed to identify deficiency and improvement opportunities within the existing security framework of T5P. These assessments will assess T5P's ability to mitigate identified information security risks from people, process and technology perspectives. These assessments will be performed by qualified individuals that have an understanding of T5P's information security environment.

When requested and for the purpose of performing internal assessments, any access needed shall be provided to members of internal assessment team. These accesses may include but not limited to:

- User level and/or system level access(es) to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective departments or administrative divisions' equipment or premises;
- Access to computer systems;
- Access to reports and documents created during internal assessment; and
- Access to interactively monitor and log traffic on networks.

Management response regarding the remedial actions of the identified issues and opportunities for improvement must be obtained.