Decision Inc. Group Information Security Policy (ISP)

The purpose of this Policy is to establish the framework for the safeguarding of the hardware, software, and information systems utilized at Decision Inc. to ensure the Confidentiality and Integrity of Company Data.

*This Policy applies to all **ITSD Resources**, whether connected to the corporate Network or not, and all Authorized Individuals whose responsibilities include inputting, safeguarding, retrieving, or using **Company Data***

AUTHORIZATION

This policy has been authorised by the Information Security Committee

AMENDMENTS

This Policy will be reviewed by the ISC on a regular basis, or as deemed appropriate based on changes in technology or regulatory requirements. Proposal for amendments to this policy should be forwarded to IT Manager: Jonathan Ferley:

RELEASE	DATE (MMYY)	AUTHOR	AMENDEMENT DESCRIPTION	Approved By
Draft	042021	JF	Policy Draft	
1.0	092021	JF	Approved Version 1.0	N Bell (ISO)

DISTRIBUTION

The distribution of this policy to recipients is controlled by the IT Manager: Jonathan Ferley. The policies will be made available through the Decision Inc. Intranet DI Connect

Table of Contents

1. Terms and Definitions

Unless specifically stated, the terms and definitions of this policy shall have the same meaning across all policies as per **Section 13, Related Policies**.

1.1. **“Account Holder”** means any staff directly or indirectly employed by decision inc. and other Account Holders affiliated with the Company who have been assigned a Company Email Account. Any employee who has been assigned a Digital Identity

1.2. **“Activation”** The implementation of disaster recovery capabilities, procedures, activities, and plans in response to an emergency or disaster declaration; the execution of the recovery plan.

1.3. **“AD”** Microsoft Active Directory

1.4. **“Alert”** Notification that a potential disaster situation exists or has occurred; direction for the recipient to stand by for possible activation of the Disaster Recovery Plan.

1.5. **“Alternate Site”** An alternate operating location to be used by business functions when the primary facilities are inaccessible.

  1.5.1. Another location, computer centre or work area designated for recovery.

  1.5.2. Location, other than the primary facility, that can be used to conduct business functions.

  1.5.3. A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster. "

1.6. **“Alternate Work Area”** Office recovery environment complete with office infrastructure (desk, telephone, workstation, and associated hardware, communications, etc.); also referred to as Work Space or Alternative Work Site.

1.7. **“Application Recovery** The component of Disaster Recovery that deals specifically with the restoration of business system software and data, after the processing platform has been restored or replaced.

1.8. **“Authentication”** means verifying the identity of a user, process, or device to allow access to a Company Information System. ITSD utilizes both Single Sign-On and Federated Identity authentication through Azure AD. Single Sign-On is when an individual uses the same DECISION INC. Login credentials to access Company Information Systems.

1.9. **“Backup Generator”** An independent source of power, usually fuelled by diesel.

1.10. **“Business Continuity Program”** An on-going program supported by executive staff and funded by the company to ensure business continuity requirements are assessed, resources are allocated, and recovery and continuity strategies and procedures are completed and tested.

1.11. **“Cold Site”** An alternate facility that already has the environmental infrastructure in place required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, communications network, etc. These must be provisioned at time of disaster.

1.12. **“Command Centre Facility”** separate from the main facility and equipped with adequate communications equipment from which initial recovery efforts are manned. The management team uses this facility temporarily to begin coordinating the recovery process until the alternate sites are functional.

1.13. **“Company Account”** Digital Identity of an Organizational User and is comprised of an email address

1.14. **“Company Data”** means anything that contains information regarding the Company made or received in connection with its operations, regardless of whether it is a hard copy or electronic, and includes, but is not limited to, written and printed matter, books, drawings, maps, plans, photographs, microforms, motion picture films, sound and video recordings, e-mails, computerized or other electronic data on hard drives or network drives, or copies of these items. See Record Retention Policy and Schedule.

1.15. **“Company Email Accounts”** means all electronic mail services provided, owned, or funded in part by the Company and operated by Decision Inc.. This term applies to processing, storage, transmission, and use of electronic mail data, including but not limited to email headers, summaries, and addresses associated with email records, attached files, or text. This term does not apply to voicemail, audio/video conferencing, or facsimile messages.

1.16. **“Company Login”** means login information provided to you by the ITSD

1.17. **“Company Network”** means the wired and wireless components and Company Technology Resources connected to the network managed by the Company.

1.18. **“Device”** means a server, computer, laptop, tablet, or mobile device used to enter or access Company Data from a Company Information System.

1.19. **“Company Information System”** means an application or software that is used to support the academic, administrative, research, and outreach activities of the Company, whether operated and managed by the Company or a third-party vendor."

1.20. **“Company-Owned Device Standard”** means the ITSD approved device configuration to be used

1.21. **“Compromised Company Email Account”** means a Company Email Account that has been maliciously broken into and could be used by an unauthorized individual for nefarious reasons.

1.22. **“Consent”** Any freely given and informed indication of an agreement by the Data Subject to the Processing of his/her Personal Information, which may be given either by a written or verbal statement or by a clear affirmative action.

1.23. **“Contact List”** A list of team members and/or key players to be contacted. (Mobile Number, Home Number etc.)

1.24. **“Corporate Network”** means the wired and wireless components and ITSD Resources connected to the network managed by the Company

1.25. **“Crisis Management Team”** A crisis management team will consist of key executives as well as key role players (i.e. legal counsel, facilities manager, disaster recovery coordinator, etc.) and the appropriate owners of critical organization functions.

1.26. **“CSIRT”** Computer Security Incident Response Team

1.27. **“Damage Assessment”** The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.

1.28. **“Data Controller”** The Decision Inc. Staff Member, usually the Representative in a Decision Inc. country office, who has the authority to oversee the management of, and to determine the purposes for, the Processing of Personal Information.

1.29. **"Data Processor"** Any Decision Inc. Staff Member or other natural person or organization, including an implementing partner or Third Party that performs Processing of Personal Information on behalf of the Data Controller.

1.30. **"Data Subject"** An identifiable natural person is one who can be identified, directly or indirectly, by reference in particular to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.31. **"Decision Inc."** means any company that is a subsidiary of Decision Inc. Holdings Proprietary Limited, whether wholly owned or partially owned. ***SIMILAR TERMS: "the Company"***

1.32. **"Declaration"** A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred, and that triggers pre-arranged mitigating actions (e.g., move to an alternate site).

1.33. **"Device"** means a server, computer, laptop, tablet, or mobile device used to enter or access Company Data from a Company Information System.

1.34. **"Digital Identity"** means the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts.

1.35. **"Disaster"** A sudden, unplanned catastrophic event causing great damage or loss. Any event that causes an organization to be unable to provide critical business functions for a pre-determined period of time.

1.36. **"Disaster Recovery"** Activities and programs designed to return Company operations to an acceptable condition. 1) The ability to respond to an interruption in services by implementing a disaster recovery plan to restore Company critical business functions.

1.37. **"Disaster Recovery Plan"** The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business disruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

1.38. **"Disaster Recovery Planning/ Business Continuity Plan (BCP)"** Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption. ***SIMILAR TERMS: "Contingency Planning", "Recovery Planning".***

1.39. **"Domain Accounts/User Accounts"** Digital Identities

1.40. **"Emergency"** A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.

1.41. **"External Email Account"** Any email account not created and issued by Decision Inc. Information Technology Services.

1.42. **"External Network"** means a network not controlled by Information Technology Services or Health Sciences Center Information Technology Services.

1.43. **"External Service Providers"** means any person not under the employment of Decision Inc. providing an approved service to the company

1.44. **"Federated Identity"** is when a Company Account Owner uses their Login to access information systems outside of the Company by establishing a trust with the Company or when the Company establishes a trust with an outside entity that provides access to Company Information Systems by individuals who do not have Decision inc. Login credentials(Guest Accounts).

1.45. **"Federated System"** means an application or software that is used to support the operations, administrative, research, and outreach activities of the Company, whether operated and managed by a third-party vendor

1.46. **"Hot Site"** An alternate facility that already has the computer, communications and environmental infrastructure in place that is required to recover critical business functions or information systems.

1.47. **"IAM"** Identity and Access Management Program

1.48. **"Identity Management"** means the creation and maintenance of the unique Company Accounts that distinguish one individual from another. IAM utilizes the following technical components to create and manage Company Accounts: Active Directory and Azure Active director.

1.49. **"Identity Provider"** means a system that creates, maintains, and management identity information while also providing authentication services to applications. Such as Azure Active Directory.

1.50. **"Illegal Activities"** means activities that break international, federal, state, or local laws such as obscenity; child pornography; threats; harassment; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; attempting to intercept any electronic communication transmission without proper authority; and violation of copyright, trademark, or defamation law.

1.51. **"Information risk owners"** means the person who is responsible for managing the information set, whom the risk is relevant to their job and has the authority to manage the threats and vulnerabilities

1.52. **"Information Service Owner"** means the person responsible for managing one or more services throughout their entire lifecycle. Service owners are instrumental in the development of application or system and are responsible for the account created for this use.

1.53. **"Internal Systems"** Federated Systems and Company Information Systems

1.54. **"ISC"** Information Security Committee

1.55. **"ITSD"** Internal IT Service Desk

1.56. **"ITSD Resources/Equipment"** means Company-owned hardware, software, and network/communications equipment, technology facilities, and other relevant hardware and software items, as well as personnel tasked with the planning, implementation, and support of technology

1.57. **"Jailbroken"** means the process of modifying an iOS device such as an iPhone, iPad, or iPod Touch to bypass restrictions imposed by Apple to allow owner to modify the operating system, install non-approved applications, and grants the user elevated administration-level privileges

1.58. **"LastPass"** means a password management tool

1.59. **"Maximum Tolerable Outage (MTO)"** The maximum tolerable outage is the amount of time the critical business functions may be without the support of IT systems and applications before business operations are severely impacted. The MTO encompasses all activities from point of impact to point of recovery.

1.60. **"Mission Critical"** means a critical task, service, or system whose failure or disruption would cause an entire operation or business to be unable to continue day to day duties

1.61. **“Off-Site Storage”** Alternate facility, other than the primary production site, where duplicate vital records and documentation may be stored for use during disaster recovery.

1.62. **“Organizational Users”** means an employee, individual the Company deems to have equivalent status of an employee but not limited to, contractors, guest researchers, and individuals from another organization or Company. ***SIMILAR TERMS: “User”***

1.63. **“Personal Information”** is any information from which a person (a Data Subject) can be identified or potentially identified from, and as such concept is defined in the Regulations.

1.64. **“Processing of Personal Information”** means any operation, or set of operations, automated or not, which is performed on Personal Information, including, but not limited to, the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer (whether in computerized, verbal or written form), dissemination or otherwise making available, correction or destruction.

1.65. **“RAO”** Resource Account Owner

1.66. **“Real-Time Scanning”** means the anti-virus software is always on and checks files in real time when they are created, opened, or copied

1.67. **“Recipient”** a natural or legal person, public authority, agency or another body, to whom the Personal Information is disclosed, whether a Third Party or not. However, public authorities which may receive Personal Information in the framework of a particular inquiry, in accordance with applicable law, shall not be regarded as Recipients; the processing of those data by those public authorities shall be in compliance with the applicable Regulations and according to the purposes of the processing.

1.68. **“Recovery Point Objective (RPO)”** The point in time to which systems and data must be recovered after an outage (e.g., end of the previous day’s processing). RPOs are often used as the basis for the development of backup strategies.

1.69. **“Recovery Time Objective (RTO)”** The period of time within which systems, applications or functions must be recovered after a disaster declaration (e.g., one business day). RTOs are often used to determine whether or not to implement the recovery strategies/plan.

1.70. **“Regulation”** this refers to both the General Data Protection Regulation of the United Kingdom, the Privacy Act No. 199, 1988 of Australia and the Protection of Personal Information Act 4 of 2013 of South Africa, as amended from time to time.

1.71. **“Remote Access”** means access to a Company Information System by a user (or a process acting on behalf of a user) communicating through an external network.

1.72. **“Remote Wipe”** means a security feature that allows data on a device be deleted without physically possessing the device

1.73. **“Representative”** means a natural or legal person established in-country who, designated by the Data Controller or Data Processor in writing pursuant to the Regulations, represents the Data Controller or Data Processor with regard to their respective obligations under the Regulations.

1.74. **“Rooted”** means the process of allowing Android users to attain privileged control over subsystems to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise inaccessible to a normal Android user.

1.75. **“Safe Haven Principles”** covers the secure storage and transfer of information.

1.76. **“SAO”** Service Account Owner

1.77. **“Sensitive Company Data”** means data identified in the Sensitive Data Protection Policy that is subject to international, federal, or state restrictions governing its processing, storage, transmission or use (e.g., personally identifiable information, credit card information, protected health information). If disclosed, Sensitive Company Data could cause significant harm to the Company or its constituents.

1.78. **“Signature Tool”** Mimecast

1.79. “**Single Sign On (SSO)”** is when a Company Account Owner uses the same Login credentials to access Company Information Systems.

1.80. **“Split Tunneling”** means the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network.

1.81. **“Staff Member** any permanent or temporary employed person contracted through any company or subsidiary of Decision Inc. Holdings Proprietary Limited. ***SIMILAR TERMS:*** *“Employee”*

1.82. **“Supported Operating System”** means the entity providing the OS, be it a vendor, open source, or an individual, is actively and routinely providing and deploying patches and security updates for the OS

1.83. **“System Owners”** means an individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system (custodian)

1.84. **“Third Party”** means a natural or legal person, public authority, agency or body, other than the Data Subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process Personal Information.

1.85. **“Two-Factor Authentication (2FA)”** means Authentication using two or more different factors to achieve Authentication, including something you know (e.g, password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).

1.86. **“Usenet Newsgroups”** means electronic discussion groups in which you can share information and opinions with people all over the world

1.87. **“Virtual Private Network (VPN)”** means a protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.

1.88. **“Warm Site”** An alternate processing site which is equipped with some hardware, and communication interfaces, electrical and environmental infrastructure which is only capable of providing backup after additional provisioning, additional software, or modifications.

2. Information Security at The Company

2.1. The Company manages information security based on the National Institute of Standards and Technology’s Cybersecurity Framework, which focuses on the following core functions:

2.1.1. Identification of cybersecurity risks to **ITSD Resources**, their capabilities, the data stored within those resources, the people who use them, and the vendors who provide them;

2.1.2. Implementation of appropriate safeguards to protect and ensure continuity of Mission Critical Services;

2.1.3. Detection of the occurrence of Security Incidents;

2.1.4. Implementation of appropriate activities to take action regarding a Security Incident or Disruption; and,

2.1.5. Planning for the efficient restoration of capabilities and functions impaired due to a Disruption.

2.2. Through carrying out the objectives outlined in this Policy, the Company seeks to encourage enterprise and innovation while also ensuring that technology risk management is a transparent, integral part of its planning, decision-making, and operations.

3. Identification Of Cybersecurity Risks

3.1. Technology policies and standards developed by **Information Security Committee** ("ISC") establishes the security posture of the Company and apply to all **ITSD Resources**, regardless of where the information or resource resides, or who manages it.

3.1.1. Individual colleges, departments, programs, and/or third-party vendors must meet the minimum security requirements but may also choose to implement more rigorous security requirements.

3.1.2. In cases of non-compliance with established Technology Governance, and **ITSD Resources** and/or Data are threatened, ISC will act to secure the resource and may limit or disconnect access to Company Network.

3.1.3. Exceptions to established Technology Governance may be granted when there is a valid justification for not being able to comply; however, because they inherently weaken the security of **ITSD Resources** and Data, exceptions will not be granted for convenience or when appropriate alternative security controls cannot be found to mitigate the risks posed.

3.2. To ensure continuity of services, a formal Business Impact Analysis ("BIA") must be completed by each Company business unit to identify the Mission Critical, Business Critical, and/or Core Services performed by it, the information system(s) that support those services, and the Maximum Tolerable Downtime ("MTD") for those systems.

3.3. All **ITSD Resources** in use must be inventoried to, at minimum:

3.3.1. Identify who owns it;

3.3.2. Establish ISC Criticality to the Company; and,

3.3.3. Ensure it is secured appropriately for the data that is processed, stored, and transmitted by it.

3.4. Purchases of new **ITSD Resources** must be compatible with the Company's existing technologies and will not impose an unnecessary risk to the Company.

3.5. Third-parties seeking to contract with the Company to perform Technology Services must complete a vendor risk assessment, provide assurances of compliance with applicable laws and regulations, and agree to adhere to established Technology Governance prior to entering into an agreement with the Company.

3.6. The Company conducts risk assessments on the following:

3.6.1. **ITSD Resources**, including specific assets or information systems;

3.6.2. Vendors of Technology Services;

3.6.3. Requests for exceptions to Technology Governance.

3.7. Additional technology risks to the Company may be identified through other activities including technology project planning, privacy impact assessments, on-site visit, whistle blowers, or self-disclosures.

3.8. All identified technology risks will be classified based on the likelihood that harm will occur as a result of the threat occurring and the harm that that may occur to the Company or individuals given the potential for the threat to exploit vulnerabilities.

3.9. Technology risks must be remediated, mitigated through implementation of compensating security controls, or accepted.

3.9.1. Accepted risks will be tracked and re-assessed annually, at a minimum, to ensure the continual risk is still in line with the Company's level of risk tolerance.

3.9.2. Aggregated data of known risks to the Company will be compiled on an annual basis and provided to Senior Management to aid in determining the Company's ongoing technology risk appetite.

4. Protecting ITSD Resources

4.1. The Company protects the Confidentiality and Integrity of Company Data by:

4.1.1. Requiring Authentication to access **ITSD Resources**;

4.1.2. Permitting Unauthenticated Access to **ITSD Resources** only in exceptional circumstances or when the resource is intended to be publicly accessible without restrictions;

4.1.3. Establishing effective on-boarding and off-boarding processes that include provisioning and de-provisioning employee access to **ITSD Resources**;

4.1.4. Basing access to **ITSD Resources** on principle of Least Privilege;

4.1.5. Securing the Company Network, including automatically blocking threats through ISC outside firewall;

4.1.6. Establishing Baseline Configurations that devices connecting to the Company Network must meet;

4.1.7. Identifying Sensitive Data stored in unsecured endpoints and remediating or securely deleting the files;

4.1.8. Physically securing facilities that house Company Data, including physical segregation within facilities when necessary;

4.1.9. Providing secure remote access to Company Information Systems; and,

4.1.10. Enforcing compliance with established Technology Governance.

4.2. The Company ensures workforce personnel secure Company Data appropriately by providing awareness on cybersecurity risk management, data protections, and duty-specific training.

4.3. To minimize the risk and impact of changes on Company business operations, all identified Mission Critical Services, Core Services, and/or **ITSD Resources** storing Sensitive Data must:

4.3.1. Establish structured, consistent change control processes;

4.3.2. Separate development and testing environments from production; and,

4.3.3. Implement High Availability, when possible.

4.4. All Company-owned devices whose use will be discontinued at the Company must be sanitized to ensure:

4.4.1. Removal of Unauthorized Access or disclosure of Sensitive Data; and,

4.4.2. Removal of Company-licensed software.

5. Threat Detection and Prevention At The Company

5.1. To identify potential internal and external threats to **ITSD Resources** and Data, the Company conducts scans, classifies, and remediates vulnerabilities.

5.2. When potential or confirmed attacks or compromises are detected, the Company will reduce or eliminate the threat through activities such as blocking or restricting access to the Company Network, disabling Company Account access, or removing the malicious content from the ITSD Resource.

5.3. The Company regularly conducts audits of Company Data Center door access logs and monitors entry doors through video surveillance or still photography to ensure only Authorized Individuals physically access Company Data Centers.

5.4. The Company will identify, detect, prevent, and respond to the warning signs of Identity Theft ("Red Flags") associated with Company Covered Accounts.

6. Security Incident Response and Recovery

6.1. All known or suspected Security Incidents must be reported to ISC immediately.

6.2. Investigation of Security Incidents will be conducted pursuant to the Incident Response (IR) Policy.

6.3. To ensure continuity of essential system functions in the event of a Security Incident or Disruption, all Mission Critical Services and Core Services must develop a Business Continuity Plan that includes the following:

6.3.1. Results of the BIA;

6.3.2. Strategies for backup and recovery of data to restore system operations quickly and effectively; and,

6.3.3. A formal Business Continuity plan (BCP) that identifies how to train personnel, activate plan, lead system recovery, and reconstitute the system after a Disruption.

7. Information Security Services Responsibilities

7.1. The Chief Information Security Officer, through Information Security committee ("ISC"), is responsible for ensuring the Confidentiality, Integrity, and Availability of ITSD Resources and Data. ISC accomplishes this mission through carrying out the following activities:

7.1.1. Developing and implementing the Technology Governance to establish the security posture of the Company;

7.1.2. Establishing a formal process for review, approval, and rescind of ITSD Resources Governance;

7.1.3. Establishing a formal process for the review, approval, and documentation of any requests for non-compliance with established Technology Governance;

7.1.4. Establishing mechanisms for tracking and enforcing compliance with applicable international, federal, and state laws and Company policies to protect Company Data;

7.1.5. Designating the appropriate level of administrative, technical, and physical security requirements for securing ITSD Resources;

7.1.6. Detecting vulnerabilities and threats to Company Information Systems and the Company Network, documenting the level of security necessary to address identified risks, and providing recommendations for the appropriate treatment of identified vulnerabilities;

7.1.7. Identifying and managing technology risks to the Company, which includes: developing processes to conduct risk assessments; ensuring identified risks are remediated;

communicating with Senior Management regarding acceptance of technology risks; and monitoring accepted technology risks over time;

7.1.8. Providing training and awareness to educate the Company community about cybersecurity risk management and data protection regulations;

7.1.9. Coordinating and overseeing risk management of and security planning activities for ITSD Resources; and,

7.1.10. Coordinating the Company's response to Security Incidents pursuant to the Computer Security Incident Response Policy.

8. Responsibilities Of Data Users and Data Stewards

8.1. Individuals who have access to Company and Client Data to perform their assigned duties or to fulfil their role within the Company community ("Data Users") are responsible for:

8.1.1. Complying with applicable international, federal, and state laws and Company policies to protect Company and Client Data;

8.1.2. Using only Company-owned, secure information systems to store and access Sensitive Data;

8.1.3. Storing Company and Client Data in a designated secure location;

8.1.4. Reporting suspected or known Security Incidents, including lost or stolen devices; and,

8.1.5. Appropriately managing all Company Data within their possession.

8.2. Senior Management who have planning and policy-level responsibilities for Company Data in their functional areas ("Data Stewards") must meet all of the responsibilities of Data Users, as well as:

8.2.1. Ensuring appropriate security controls are in place to protect the data they oversee;

8.2.2. Authorizing and de-authorizing access to data under their stewardship, based on the principle of Least Privilege;

8.2.3. Ensuring individuals granted access to data are appropriate trained to comply with the applicable international, federal, and state laws and Company policies to protect the data;

8.2.4. Establishing the Company's technology risk tolerance by:

8.2.4.1. Remediating and/or mitigating any risks or gaps identified as a result of risk assessments or compliance checks within the areas they oversee;

8.2.4.2. Elimination and/or mitigation of security vulnerabilities from the ITSD Resources they oversee; and,

8.2.4.3. Accepting any technology risks associated with their areas of responsibility.

9. Awareness raising

In connection with the implementation of this policy, ISC shall hold periodic training and awareness raising sessions throughout DECISION INC. in partnership with regional offices. Key users are encouraged to attend these sessions.

It is the responsibility of key users to take privacy and security into consideration when evaluating the potential the use of cloud-based IT services. In addition, staff that grant access to DECISION INC. ITSD systems need to ensure that authorized users are aware of this policy.

10. Enforcement & Interpretation

10.1. Any staff who violates this Policy shall be subject to appropriate disciplinary action.

10.2. Any other Account Holder who has a Company Email Account and violates this Policy shall be subject to appropriate corrective action, including, but not limited to, termination of their relationship with the Company.

10.3. The Company Chief Information Officer, supported by the Chief Information Security and Privacy Officer, will coordinate with appropriate Company entities on the implementation and enforcement of this Policy.

10.4. Responsibility for interpretation of this Policy rests with the Chief Information Officer.

11. Breaches Of Policy

11.1. Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Company assets, or an event which is in breach of the Company's security procedures and policies.

11.2. All Company employees, elected members, partner agencies, Third Parties and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Company's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Company.

11.3. The Company will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the disciplinary procedure

12. Review Of Policy

12.1. An annual review of the information security policy must be conducted. The information security committee is responsible for managing the review process. Changes to the policy must be presented to and approved by a majority of the ISC and the information necessary to measure the organizations' adherence to the information security policy objectives and the maturity of the information security program.

13. Related Policies

13.1. Decision Inc. Group Access Control Policy (ACP)

13.2. Decision Inc. Group Email Communication Policy (ECP)

13.3. Decision Inc. Group Personal Data Protection Policy

13.4. Decision Inc. Group Identity Access and Management Policy (IAM)

13.5. Decision Inc. Group Incident Response Policy (IR)

13.6. Decision Inc. Group IT Operations and Administration Policy

13.7. Decision Inc. Group Personal and Mobile Device Policy (BYOD)

13.8. Decision Inc. Group Remote Access Control Policy (RACP)

13.9. Decision Inc. Group Information Handling and Classification Policy

13.10. Decision Inc. Group Acceptable Use Policy (AUP)

13.11. Decision Inc. Group Change Management Policy