launchpad

Launchpad Technologies Inc.

INFORMATION SECURITY POLICY

POLICY VERSION	V2.3
EFFECTIVE DATE	March 18, 2018
REVISION DATE	January 19, 2019

Purpose and Objectives:

The Information Security Policy (ISP) establish Launchpad Technologies Inc.'s ("Launchpad") corporate approach to information security management. The Information Security Policy acts as the framework under which all personnel must operate in order to ensure the information security practices at Launchpad are reasonable, appropriate, and efficient. This in return will ensure the reasonable protection of personal and confidential information in a manner that is compliant with the security requirements of the Freedom of Information and Protection of Privacy Act and the Information Management Act.

Scope:

This policy applies to all full-time, part-time, or contract personnel at Launchpad Technologies.

Roles and Responsibilities

The Launchpad Executive Team and the departmental managers share responsibility for providing corporate strategies, policies, standards and guidelines on information security.

The Executive Team must:

(a) Maintain and review annually the Information Security Policy; and

(b) Advise departmental managers of any changes to the Information Security Policy.

(c) Provide cross-departmental leadership for information security;

(d) Manage the corporate information security risks;

(e) Establish a program to manage and coordinate information security activities;

(f) Monitor for, assess, and respond to, information security threats and exposures;

(g) Provide evidentiary support and analysis of digital evidence in support of suspected or actual information incidents; and

(h) Assist departments in performing information security activities.

Departmental managers must:

(a) In collaboration with the Executive Team, develop and maintain security controls to protect the confidentiality, integrity and availability of information, throughout its lifecycle;

(b) Ensure promotion of information security initiatives within their department;

(c) Employ appropriate controls to reduce the risk of disruption of information systems such as unauthorized or unintentional modification or misuse of information systems; and

(d) Integrate information security into the organization's project management and change management processes to identify and address information security risks.

1. PERSONNEL SECURITY – This section identifies security responsibilities and management processes throughout the employment cycle.

Supervisors must ensure:

(a) Prior to employment, employee security screening is done in accordance with Launchpad policies and practices;

(b) During employment, employees are informed about the information security policies and procedures, Information Security roles and responsibilities;

(c) At termination, employees are reminded of their ongoing confidentiality responsibilities following termination of employment;

(d) Potential or actual information security breaches are investigated and reported, and invoke incident management processes where necessary; and

(e) Contractor responsibilities for information security are identified in contractual agreements.

2. MANAGEMENT OF INFORMATION SYSTEMS AND DEVICES – This section defines requirements for secure management of Launchpad systems and devices.

Departmental Managers must:

(a) Maintain an inventory of Launchpad systems and devices, including portable storage devices, and all mobile devices;

(b) Validate the measures taken to protect information systems and devices as part of an enterprise risk management strategy. This includes maintaining, documenting, verifying and valuing asset inventories on a regular basis;

(c) Document the return of devices in the possession of employees upon termination of their employment;

(d) Remove information from devices that are no longer needed by Launchpad; and

(e) Securely dispose of devices in a manner appropriate for the sensitivity of the information the device contained. Mobile device users must lock and/or secure unattended mobile devices to prevent unauthorized use or theft.

3. ACCESS TO INFORMATION SYSTEMS AND DEVICES - This section identifies security roles, responsibilities and management processes relating to access and authorization controls for Launchpad systems and devices.

Departmental Managers must define, document, implement, communicate and maintain procedures to ensure access to Launchpad systems and devices are granted to individuals based on business requirements and the principles of “least privilege” and “need-to-know.”

Supervisors must:

(a) Ensure the assignment and revocation of access rights follow a formal and documented process;

(b) Regularly, and upon change of employment, review, and update where appropriate, employee access rights to ensure they are up to date. Employees must know and adhere to password security practices.

4. ENCRYPTION - This section defines encryption methods for improving the protection of information and for reducing the likelihood of compromised sensitive information.

The Executive Team must:

(a) Provide direction and leadership in the use of encryption and the provision of encryption services, including those used for user registration; and

(b) Set corporate direction for the management (generating, storing, archiving, distributing, retiring and destroying) of encryption keys throughout their lifecycle. The Executive Team supports, and provides advice on, the use of encryption technologies.

Departmental Managers must:

(a) Select information encryption controls during system design to provide appropriate protection commensurate to the information value and security classification; and

(b) Register the use of encryption technology products and services with the Executive Team.

5. PHYSICAL AND ENVIRONMENTAL SAFETY - This section identifies operational requirements for protecting facilities where Launchpad information and information systems are located.

Departmental Managers must:

(a) Design, document and implement security controls for a facility based on an assessment of security risks to the facility;

(b) Review, and where appropriate test, physical security and environmental control requirements;

(c) Establish appropriate entry controls to restrict access to secure areas, and to prevent unauthorized physical access to information and devices;

(d) Incorporate physical security controls to protect against natural disasters, malicious attacks or accidents; and

(e) Ensure security controls are maintained when computer equipment, information or software is used outside Launchpad facilities.

6. OPERATIONS SECURITY - This section establishes a framework for identifying requirements to control, monitor, and manage information security changes to the delivery of Launchpad services.

Departmental Managers must:

(a) Plan, document and implement change management processes to ensure changes to information systems and information processing facilities are applied correctly and do not compromise the security of information and information systems;

(b) Monitor and maintain information systems software throughout the software lifecycle;

(c) Define, document, assess, and test backup and recovery processes regularly;

(d) Implement processes for monitoring, reporting, logging, analyzing and correcting errors or failures in information systems reported by users and detection systems;

(e) Ensure operating procedures and responsibilities for managing information systems and information processing facilities are authorized, documented and reviewed on a regular basis;

(f) Establish controls to protect log files from unauthorized modification, access or disposal;

(g) Establish processes to identify, assess, and respond to vulnerabilities; and (h) Enable synchronization of computer clocks to ensure integrity of information system logs and accurate reporting. The Executive Team must assess, provide advice, monitor response progress, and report on vulnerability response activities.

7. COMPUTER NETWORK AND COMMUNICATION SECURITY - This section identifies requirements for the protection of sensitive or confidential information on computer networks.

The Executive Team must provide direction and leadership on implementation of, and significant modification to, electronic messaging systems. The Executive Team must develop corporate security controls to protect information from interception, copying, misrouting and unauthorized disposal when being transmitted electronically.

Departmental Managers in collaboration with the Executive Team must:

(a) Document network security controls prior to commencement of service delivery;

(b) Ensure security features are implemented prior to commencement of service delivery;

(c) Document, implement and manage changes to network security controls and security management practices to protect Launchpad information systems from security threats;

(d) Ensure segregation of services, information systems, and users to support business requirements based on the principles of least privilege, management of risk and segregation of duties;

(e) Ensure implementation of network controls to prevent unauthorized access or bypassing of security control;

(f) Ensure electronic messaging services are protected commensurate to the value and sensitivity of message content, and approved for use by the Executive Team.; and

(g) Ensure information transfers between Launchpad and external parties are protected using services approved for use by the Executive Team.

8. WORKING REMOTELY - This section defines information security requirements that apply to employees working remotely.

Departmental Managers must:

(a) Ensure that Launchpad information and devices are protected regardless of the type of access or physical location of employees; and

(b) Develop and communicate policies and processes specific to their areas that govern occasional teleworking that may not have a formal agreement in place.

9. INFORMATION SYSTEM PROCUREMENT, DEVELOPMENT AND MAINTENANCE - This section defines requirements to ensure security controls are included in business and contract requirements for building and operating secure information systems, including commercial off the shelf and custom-built software.

Departmental Managers must:

(a) Develop, implement and manage the processes and procedures necessary to ensure that information security risks and privacy requirements are taken into account throughout the systems development lifecycle;

(b) Ensure sufficient resources and funding are allocated to complete the necessary information security tasks;

(c) Ensure that system development or acquisition activities are aligned with Launchpad information security requirements and standards;

(d) Apply vulnerability scanning, security testing, and system acceptance processes commensurate to the value and sensitivity of the information system. The Executive Team must provide corporate direction and oversight for developing and implementing security standards to procure, develop and maintain information systems.

10. SUPPLIER RELATIONSHIPS - This section defines requirements to ensure supplier agreements for information systems and cloud services align with Launchpad security policies, standards and processes.

Departmental Managers must:

(a) Ensure identified security requirements are agreed upon and documented prior to granting external parties access to information, information systems or information processing facilities;

(b) Ensure security controls, service definitions, and delivery levels are identified and included in agreements with external parties prior to using external information and technology services;

(c) Establish processes to manage and review the information security controls of services delivered by external parties, on a regular basis;

(d) Ensure that changes to the provision of services by suppliers of information system services take into account the criticality of the information and information systems involved and the assessment of risks;

(e) Assess business requirements and associated risks related to external party access to information and information systems; and

(f) Ensure the risks of external party access to information and information systems are identified, assessed, mitigated and managed.

11. CLOUD SERVICES SECURITY - The Executive Team provides corporate direction and leadership on the secure use of cloud services by:

(a) Establishing policy and providing strategic direction on the use of cloud services;

(b) Establishing roles and responsibilities;

(c) Establishing information security requirements for cloud services.

Departmental Managers must:

(a) Notify the Executive Team prior to procuring cloud services; and

(b) Consider existing cloud service offerings prior to procuring new cloud services

12. INFORMATION INCIDENT MANAGEMENT - This section addresses the response and management of information incidents, including privacy breaches, in order to take the appropriate steps to mitigate the risk of harm.

Employees must immediately report suspected or actual information incidents. Departmental Managers must establish specific information incident management policies and procedures, as appropriate, to ensure quick, effective and orderly response to information incidents within the organization.

13. BUSINESS CONTINUITY MANAGEMENT – This section defines requirements to prepare, and re-establish, business or services as swiftly and smoothly as possible in adverse situations.

Departmental Managers must:

(a) Establish, document, implement, and maintain processes, procedures and controls to ensure the required level of information security for business continuity and disaster recovery during an adverse situation;

(b) Ensure that vital records and critical systems are identified in business continuity plans;

(c) Review business continuity and recovery plans annually to ensure they are current, valid, functional and readily accessible during a business interruption; and

(d) Regularly conduct business continuity and recovery exercises and, where necessary, update business continuity and recovery plans.

14. ASSURANCE AND COMPLIANCE - This section defines requirements to ensure compliance with legislation, government policies and standards.

The Executive Team must:

(a) Initiate an independent review of the overall Launchpad information security program on a regular basis; and

(b) In collaboration with departments, report on each one's adherence to the information security policies, and standards.

Departmental Managers must:

(a) Ensure the regulatory and contractual security requirements of information systems are identified, documented, addressed and maintained; and

(b) Regularly review information systems and information security procedures to ensure compliance with security policies and standards.