INFORMATION SECURITY POLICY

Document Version 1.0

Date: October 2 2017

TABLE OF CONTENTS

1 PURPOSE / OBJECTIVE

1.1 INFORMATION SECURITY

The security of the services provided by or to and of the private and personal information entrusted to LogicalOutcomes is critical to the organization's success and the strategic objective of improving the efficiency and effectiveness of LogicalOutcomes' evaluation services.

Loss of confidentiality, integrity, or availability of information, or of the technology-based systems and services, could adversely affect the achievement of LogicalOutcomes' goals and objectives, and result in harm to LogicalOutcomes, its clients, and other stakeholders.

Information security is the discipline that assists in identifying and mitigating security-related risks to limit potential damages; and to enable the achievement of business objectives.

LogicalOutcomes uses a risk based approach towards Information Security. Risks are evaluated based on how they may impact the organization, and will be re-evaluated as security safeguards are added.

1.2 PURPOSE

This policy represents the Board of Directors' commitment to Information Security in the organization.

This policy provides direction to LogicalOutcomes Personnel on the security of organizational assets, including but not limited to information, including Personal Health Information (PHI), Personal Information (PI) and other Agency Information, services, and information technology resources to guard against theft, loss, unauthorized use, disclosure, disruption, modification or disposal.

1.3 OBJECTIVES

This policy is intended to ensure:

1) The establishment of accountabilities and implementation of safeguards that are consistent with the responsibilities placed upon LogicalOutcomes under the roles that the organization could play, as defined under the Personal Health Information Protection Act, 20043 (PHIPA) and O. Reg. 329/04 ("the Regulation") as amended from time to time;
2) That security mechanisms and practices will be employed to protect information collected, used, stored, transmitted, disclosed or exchanged by the organization, and to ensure the continued delivery of services through the use of information systems;
3) The consistent and effective management of safeguards throughout LogicalOutcomes through the implementation of security plans, practices, and controls in alignment with ISO 27001 Information Security Management Systems Requirements.

2 SCOPE

2.1 SCOPE AND APPLICABILITY

This Policy will be the foundational component of LogicalOutcomes' security governance and accountability framework.

This policy applies to all LogicalOutcomes Personnel, including paid consultants and volunteers.

This Policy applies to all:

1) LogicalOutcomes business units and program areas.
2) Information owned or controlled by LogicalOutcomes, or for which the organization has a stewardship responsibility;
3) Assets and facilities owned, leased, licensed, or managed by LogicalOutcomes;
4) Information security services provided by LogicalOutcomes, both internally and externally; and
5) Information security services provided by public or private sector organizations to LogicalOutcomes, and relied upon by the organization for the conduct of its business.

2.2 VIOLATIONS

Violation of the policy by Personnel may result in disciplinary action, up to and including termination. Violation of the requirements of this policy by a service provider may be subject to the penalties contained within any contractual agreement between LogicalOutcomes and the service provider.

3 PRINCIPLES

The following principles guide this policy:

3.1 GOVERNANCE

i. Information security will ensure the confidentiality, integrity, and availability of organizational Assets, including information systems and information entrusted to LogicalOutcomes;
ii. Security of Assets will be approached in a holistic and practical manner throughout the Asset lifecycle;
iii. Information security strategies, mechanisms, and competencies will be regularly reviewed to ensure compliance, suitability, and effectiveness;
iv. Continuous information security awareness, education and training should be practiced.

3.2 CONTROLS

i. Information security requirements must be documented and will be enforced;
ii. Safeguards must be applied in a manner consistent with business requirements and best practices, and compliant with policy, legal and regulatory requirements;
iii. Safeguards consist of people, processes and technology;
iv. Responsibilities / duties assigned to individuals must follow the principle of “segregation of duties” and “least privilege”.

3.3 RISK

i. Information security risks must be identified, evaluated, and treated / escalated according to the Enterprise Risk Management Policy; or Corporate Compliance Policy as required;

ii. Information security risks must be documented and communicated to the appropriate stakeholders;
iii. Infrastructure or enterprise risks identified during an application Threat and Risk Assessment (TRA) must be managed by the appropriate infrastructure or enterprise stakeholder;
iv. Information security-related business residual risks must be managed and accepted at the appropriate level within LogicalOutcomes

4 POLICY

4.1 GENERAL

Confidentiality, integrity, and availability safeguards for information, and information systems and resources must be designed to comply with applicable requirements, including but not limited to legislative requirements (e.g., PHIPA and the Regulation) and agreements entered into between LogicalOutcomes and external parties.

All Information and Information Technology (I&IT) assets (Physical & Data) must be classified and protected according to the LogicalOutcomes Information Classification Standard Practice. Business owners are responsible for identifying and classifying I&IT Assets used by their area.

All I&IT Assets must be secured in line with legal and business requirements throughout the Asset lifecycle. Evaluation and selection of information security controls for Sensitive Assets must include the following domains when applicable:

a. Asset management;
b. Human resource security;
c. Physical and environmental security;
d. Secure communications and operations management;
e. Access control;
f. System development and acquisition;
g. Security incident management;
h. Business continuity management; and
i. Security compliance.

The rationale and approval for the exclusion of any of the above domains from an assessment shall be documented.

All new and existing business units shall be assessed for security requirements.

New programs and projects will identify security requirements that must be included in its deliverable design. Security requirements must be documented to the same level of granularity as the deliverable requirements. Where applicable, these security requirements will be included in the solution documentation for review by LogicalOutcomes' architecture gating bodies.

The design of information systems and resources must:

a. Comply with PHIPA and the Regulation, other applicable laws, and any other applicable legal requirements (such as agreements entered into between LogicalOutcomes and external parties);
b. Comply with LogicalOutcomes privacy and security policies and standards;
c. Align with security best practices;
d. Include processes that record information about security incidents and communicate that information to the appropriate stakeholders;
e. Include processes and technology to monitor the security of information systems and resources; and
f. Include supporting materials to demonstrate compliance with this policy. Safeguards must be planned, documented, implemented, and tested.

New or modified safeguards must be recorded, evaluated, and approved by the appropriate stakeholder(s), before those safeguards are implemented, changed or deleted.

Safeguards that do not successfully pass testing:

a. Will not be considered as safeguards as intended; and
b. Must be recorded, re-evaluated, and re-assessed for risk treatment by the appropriate stakeholder(s).

Where possible, technical security controls must be auditable.

Technical security controls will be reviewed periodically to verify that they continue to operate as planned.

Business unit managers must ensure that all security responsibilities within their area are carried out correctly and in a manner that complies with applicable security requirements.

All areas within the organization will be subject to regular audit to ensure compliance with applicable security requirements.

Compliance with the requirements of this policy will be subject to internal audit.

4.2 Personal Health Information and Personal Information

LogicalOutcomes must comply with the requirements of PHIPA and the regulation, and any other applicable laws for personal health information (PHI), Personal Information (PI) and other records. This includes, but is not limited to, the following mandatory requirements:

a. Ensuring the necessary written agreements are executed and maintained where required under law or as a best practice;
b. Keeping an electronic record of all accesses to PHI maintained by LogicalOutcomes;
c. Performing a security threat risk assessment (“TRA”) with respect to threats, vulnerabilities and risks to the confidentiality, availability and integrity of the data, information system, service or resource dealing with PHI and on request, making available a written copy of the summary of the TRA to each health information custodian that provides PHI to LogicalOutcomes;
d. Describing the administrative, technical and physical safeguards relating to the confidentiality, integrity and availability of the personal health information as appropriate.

Personnel within LogicalOutcomes will treat and handle PHI in accordance with PHIPA and the Regulation. This includes the following compulsory requirements:

a. Having proper authorization and written agreement from the Chief Privacy Officer before accessing or handling PHI;
b. Protecting the integrity, availability and confidentiality of PHI; and
c. Immediately reporting potential unauthorized access / handling or loss of PHI to your respective Project Manager and then the Executive Director in accordance with LogicalOutcomes' Incident Management policy.

4.3 Security Risk Management

Security assessments must be performed on Sensitive Assets to identify risks. These assessments must be performed periodically, or on notice of significant change.

Security risks will be evaluated with risk treatment options.

The treatment and acceptance of security risks must align with LogicalOutcomes' governance and Enterprise Risk Management Policy.

Residual security-related business risk(s) must be accepted by a person with the necessary authority (e.g., Risk Owners) within the organization.

The Executive Director, with input from the Ethics and Privacy Subcommittee of the Board, must create and maintain a security plan for Sensitive Assets. The security plan must document at least the following:

a. Appropriate management action, resources, responsibilities and priorities to mitigate identified security risks;
b. The confidentiality, integrity and availability safeguards selected and their implementation plans;
c. the level of risk accepted;
d. The routine review of compliance to applicable security requirements; and
e. The routine review and improvement of safeguard effectiveness.

Security plans shall be signed by the Executive Director or President of the Board.

4.4 External Parties

When exchanging information with external organizations, or relying on information technology infrastructure and services provided by other parties, or an external party accessing agency information or processing facility, LogicalOutcomes must establish written contracts and legal service agreements with these organizations which must include security controls that meet or exceed the requirements of this Policy.

Where an external party has a standard agreement and no provision to vary it to meet agency requirements, the external party's standard clauses are assessed against LogicalOutcomes' requirements and the risk associated with the gap is assessed before deciding whether or not to proceed with the offered terms. Where there is a significant variation between the requirements

and what is offered, the security services risk management process will be followed in order to proceed with the provider as governed by Enterprise Risk Management Policy.

Existing contracts and service agreements that do not meet or exceed the requirements of this policy must be updated for compliance at the earliest reasonable time e.g. on contract renewal negotiation. Where necessary, a nondisclosure agreement must be entered with the third party. Access to existing and new processing facilities must follow the process identified under Physical and Environmental Security Policy.

4.5 Accountability

Any individual who causes or contributes to a Security Incident will be held accountable when his / her action or inaction goes against training received, job specification, agreement, contract, policy, or law.

5 Responsibilities

5.1 LogicalOutcomes Board of Directors

The LogicalOutcomes Board of Directors will be responsible for:

a. Review and approval of this Policy;
b. Oversight of LogicalOutcomes' capability for security risk management; and
c. Being informed of significant security risks related to the organization, and actions being taken by management to ensure risks are managed within the acceptable risk tolerance levels.

5.2 Executive Director (ED)

The ED will be responsible for:

a. Ensuring that all LogicalOutcomes Personnel have a clear understanding of security expectations for which they will be held accountable;
b. Ensuring that appropriate structures and processes are in place for the execution of the organization's security governance and accountability framework;
c. Ensuring that all LogicalOutcomes Personnel comply with the principles and mandatory requirements of corporate management policies and standards and laws;
d. Maintaining relationship with the LogicalOutcomes' Board of Directors, and communicating the Board's directions with regard to risk tolerance and security risk management expectations; and
e. Accepting residual security-related business risks as required.

5.3 Project Owner

The Project Owner of each project is responsible for:

a. Ensuring compliance with the requirements in this policy;
b. Accepting residual security-related business risks within the appropriate level of authority;
c. Approving the project's security plans;

d. Providing business directions and confirming business priorities in regards to the project's security plan;
e. Communicating the ED's directions with regard to risk tolerance and security risk management expectations; and
f. Approving adequate funding and resources for the project's security plans.

5.4 Project Managers

The Project Managers shall be responsible for:

a. Providing direction and oversight for management of security risks within their areas of responsibility;
b. Ensuring that all business operations and service delivery requirements follow this policy, and the security policies and standards of the organization;
c. Routinely reviewing compliance with the requirements in this policy;
d. Ensuring that adequate procedures, training and awareness programs are attended to make all employees, contractors and vendors' employees aware of their Information Security obligations;
e. Developing and executing the business unit's security plan(s); and
f. Ensuring that all employees, contractors or third party users under their responsibility: return Agency assets in their possession upon termination of their employment, contract or agreement; and all the access rights and authorization are removed from the systems.

5.5 Chief Security Officer, Security Services

The Chief Security Officer, Security Services is responsible for:

a. This policy, as well as other security policies;
b. Approving routine compliance reviews of business unit security plans;
c. Approving the information security governance and the Security Services Department's plan;
d. Ensuring that LogicalOutcomes' information security plan is coordinated with, and has business objectives consistent with the organization's privacy plans;
e. Providing corporate leadership and direction to business units on the implementation of this policy; and
f. Coordinating responses to information security issues at the overall organization level.

5.6 Legal

The Legal department is responsible for:

a. Reviewing this policy;
b. Maintaining the contact list with authorities that may be used in the event of a security incident; and
c. Ensuring necessary review is conducted before contacting authorities.

5.7 Security Services

Security Services is responsible for:

a. Evaluating the effectiveness of this and other security policies, and recommending any necessary changes to the policy;
b. Coordinating routine compliance reviews of business unit security plans;
c. Developing and managing information security governance and Security Services Department's plan;
d. Developing the organization's information security training and awareness program; and
e. Providing information and advice to the business units to ensure consistent implementation of safeguards and security plans.

5.8 Personnel (including Agency and third party Service Providers)

Personnel are responsible for:

a. Completing the annual security training and awareness program;
b. Reading, understanding, accepting and signing the Employee Privacy and Security Code of Conduct or the Privacy and Security Standard of Conduct for Service Providers, as applicable;
c. Reading, understanding, accepting and signing the Acknowledgment of Confidentiality; reading, understanding, and accepting the Information and Information Technology (I&IT) Resource Acceptable Use policy; and
d. Following all LogicalOutcomes security policies, standards and procedures.

5.9 Procurement

The Procurement department is responsible for:

a. Ensuring all contractors and agents have undergone necessary screening, as per the Security Screening Policy; and
b. Working with Security Services and Legal to ensure appropriate language is included in contracts and Requests for Proposal (RFPs).

6 GLOSSARY

TERM DEFINITION

Accountability Any individual who causes or contributes to a Security Incident will be held accountable when his / her action or inaction goes against training received, job specification, agreement, contract, policy, or law.

Approver The individual responsible for ensuring that the policy, process, procedure, etc. is defined and maintained to serve (related) business objectives effectively. This may (typically) also be the owner.

Asset A component or part of the total system or network to which the owner directly assigns a value to represent the level of importance to the "business" or operations/operational mission of the Business Unit, and therefore warrants an appropriate level of protection.

Asset types include, but are not limited to: information, hardware, communications equipment, firmware, documents/publications, environmental equipment, infrastructure, money, revenue, services and organizational image.

Availability The property of an asset and services that ensures they can be accessed and used as required, without undue delay.

Business Unit A group of people within LogicalOutcomes, including but not limited to a division, department, program, or project.

Business Unit Head A head of a Business Unit within LogicalOutcomes, e.g., Operations, Development and Delivery, etc.

Confidentiality The property that information is available or disclosed only to authorized individuals, entities or processes.

Document Prime The individual responsible for managing and maintaining the process document, and who is the focal point for questions and information pertaining to the document. Typically, this is a Subject Matter Expert (SME), and may participate in or guide the development of the process document.

Integrity The assurance that the information being used, displayed or sent has not been modified by unauthorized means.

Owner The individual – designated by management – responsible for the development, maintenance, and communication of the policy, process, procedure, etc. to achieve (related) business objectives in an effective and efficient manner.

Personnel LogicalOutcomes staff (contractors, temp agency staff, co-op students and seconded individuals, volunteers.)

Personal Health Information Has the meaning set out in section 4 of the Personal Health Information Protection Act, 2004 (PHIPA), and generally means identifying information about an individual in oral or recorded form pertaining to that person's health or health services provided to the individual.

Personal Information (PI) Has the meaning set out in section 2 of the Freedom of Information and Protection of Privacy Act (FIPPA) as: recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, telephone number, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they relate to another individual, (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, and (h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual.

Risk Treatment Action(s) that may be taken to bring the risk situation to a level where the exposure to risk is acceptable to LogicalOutcomes.

Safeguard A precautionary measure, stipulation, device, technical or non-technical solution to prevent an undesired incident from occurring.

Security Incident Any activity that could compromise the security of sensitive personal information or systems, including but not limited to, a social engineering attempt such as a request for a password, loss of a laptop or blackberry, a computer virus infection, degradation of a system, unauthorized changes to files or file sizes, or the addition of files.

Sensitive Asset Any Asset defined as sensitive in accordance with the Information Classification Policy.

Sensitive Information Information defined as sensitive in accordance with the Information Classification Policy.

Service Provider An individual or entity that LogicalOutcomes contracts to act on the Agency's behalf to provide goods or services that assist in the delivery of LogicalOutcomes Services. The term includes vendors, consultants and service delivery partners.

User All LogicalOutcomes Personnel and anyone else who is granted access to LogicalOutcomes information, systems and other IT resources.

7 REFERENCES AND ASSOCIATED DOCUMENTS

REFERENCE LOCATION

Development Corporations Act
http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_90d10_e.htm

Freedom of Information and Protection of Privacy Act
http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm

Personal Health Information Protection Act, 2004
http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

eHealth Ontario Information Security Policy (Document Version 1.0)