INFORMATION SECURITY POLICY

Effective date: September 27, 2018

Version	Description	Reason for revision	Approved by Board
1.0	First information security policy	N/A	October 17, 2017
1.1	Current draft – 2018-Sept-06	Major revisions aimed at compliance with GDPR and consistency with other LogicalOutcomes policies	September 27, 2018

SCHEDULED REVIEW DATE: September 27, 2020

TABLE OF CONTENTS

1 Policy Statement

This policy provides direction to LogicalOutcomes personnel on the security of information assets. It addresses the privacy of personal health information and personal information as well as the integrity and availability of all our information assets against theft, loss, unauthorized use, disclosure, disruption, modification or disposal.

2 Purpose

The privacy of the private and personal information entrusted to LogicalOutcomes is critical to our mission. While this information security policy addresses protection against the loss of all types of business information (including financial and project management data), the policy is primarily focused on protecting personal information that is collected in our monitoring and evaluation projects.

The approach we used in developing the Information Security Policy is described in the SIS Security White Paper[1]. It is guided by the Principles for Digital Development[2] and the aim of compliance with the European Union General Data Protection Regulation (GDPR).

According to the GDPR[3], the protection of personal information requires that we:

- design and organise our security to fit the nature of the personal data we hold and the harm that may result from a security breach;
- have a process in place to ensure that information security related policies and procedures are reviewed and approved before implementation;
- be clear about who in our organisation is responsible for ensuring information security;
- make sure we have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff;
- be ready to respond to any breach of security swiftly and effectively;
- and review and update policies and procedures in line with agreed timescales or when required.

By complying with the GDPR, LogicalOutcomes will also comply with its responsibilities under the Personal Health Information Protection Act (PHIPA) and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA).

3 Scope

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

The policy applies to all:

[1] See Reference section
[2] See the Principles for Digital Development at https://digitalprinciples.org/principles/
[3] The following points are paraphrased from https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

a. LogicalOutcomes business units, program areas and projects;
b. Information owned or controlled by LogicalOutcomes, or for which the organization has a stewardship responsibility;
c. Assets and facilities owned, leased, licensed, or managed by LogicalOutcomes;
d. Information security services provided by LogicalOutcomes, both internally and externally; and
e. Information security services provided by public or private sector organizations to LogicalOutcomes, and relied upon by the organization for the conduct of its business.

The policy does not apply to information that is collected and managed by clients of LogicalOutcomes.

4 RESPONSIBILITIES

This section outlines the responsibilities of the board, management and other personnel in regards to the policy as well as who is responsible for developing, maintaining, monitoring and implementing the policy.

Failure to comply with the policy by LogicalOutcomes personnel, including consultants, contractors, students and volunteers, may result in termination of the person's or company's relationship with LogicalOutcomes.

4.1 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.

4.2 LOGICALOUTCOMES ETHICS AND PRIVACY COMMITTEE

The LogicalOutcomes Ethics and Privacy Committee, as a standing Committee of the Board, will be responsible for:

a. Review of draft policies and procedures before their presentation to the Board for approval;
b. Advising the Board regarding security, privacy and ethical issues relating to personal information.

4.3 EXECUTIVE DIRECTOR

The Executive Director 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; and

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.

4.4 Project Managers

The Project Managers shall be responsible for the following, within the projects they manage:

a. Setting up and managing projects in accordance with this policy and its associated procedures;
b. Routinely reviewing compliance with the requirements in this policy;
c. Ensuring that project team members have adequate training and awareness regarding their Information Security obligations; and
d. Ensuring that access rights and authorization for Internal and Confidential project information are removed for all personnel or third party users under their responsibility.

4.5 Security/Privacy Officer

The Security/Privacy Officer is responsible for:

a. This policy, as well as other security policies and procedures;
b. Approving routine compliance reviews of project security plans;
c. Ensuring that LogicalOutcomes' information security policy is coordinated with, and has business objectives consistent with the organization's privacy policy;
d. Providing corporate leadership and direction to business units and projects on the implementation of this policy;
e. Acting as the LogicalOutcomes Privacy Officer, being the first point of contact for privacy issues raised by LogicalOutcomes personnel, clients and web site users; and
f. Coordinating responses to information security issues at the overall organization level.

4.6 Data Protection Officer (DPO)

The Data Protection Officer is responsible for[4]:

a. Informing and advising LogicalOutcomes and its personnel about their obligations to comply with the GDPR and other data protection laws;
b. Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, reviewing training processes, and conducting internal audits;
c. Being an escalation point of contact for supervisory authorities and for individuals whose data is processed (personnel, clients etc.) if the Security Officer/Privacy Officer has not resolved an issue.

4.7 Personnel (including Consultants and third party Service Providers)

Personnel are responsible for:

a. Completing an annual security training and awareness program;
b. Reading, understanding, accepting and signing a confidentiality agreement;

[4] Paraphrased from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

c. Following all LogicalOutcomes information security policies, standards and procedures.

5 DEFINITIONS

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 department, program, or project.

Information Classifications The classification of LogicalOutcomes information assets according to four categories: Internal, Open access, Confidential-Organization and Confidential-GDPR:

- **Internal** The default classification for Information that is managed by LogicalOutcomes, including drafts, notes, background documents and reports that should not be publicly available but that would not cause serious harm if they were mistakenly shared with the wrong people.
- **Open Access** Information that may be made freely available to the community through Creative Commons licenses.
- **Confidential-Organization** Any business information that is defined as Confidential by LogicalOutcomes or a client organization and that is not personal information.
- **Confidential-GDPR** Any information that is defined as personal under GDPR, which is essentially the same as personal information, defined below.

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

Personnel Any person working on LogicalOutcomes projects and under the management control of LogicalOutcomes, including consultants, staff of third party service providers, students, interns and seconded individuals and volunteers. It does not include people working under the management control of client organizations.

Personal Health Information Has the meaning set out in section 4 of the Ontario 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 Ontario 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 mobile device, a computer virus infection, degradation of a system, unauthorized changes to files or file sizes, or the addition of files.

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.

6 REFERENCES

eHealth Ontario Information Security Policy (Document Version 1.0)
http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecPolicy_EN.pdf
(We excerpted several relevant sections from the eHealth Ontario policy, by permission, in this Information Security Policy.)

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

General Data Protection Regulation (GDPR) (European Union)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
See the UK Information Commissioner's Office guidelines at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ for a more usable set of resources.

Microsoft Compliance Manager for GDPR
https://servicetrust.microsoft.com/ComplianceManager

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

Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Principles for Digital Development
https://digitalprinciples.org/principles/

Guide to Data Protection – Information Security - Information Commissioner's Office (UK)
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

SIS Security White Paper (LogicalOutcomes)
https://zenodo.org/record/1211680#.W0ZyCNJKhPY

7 PROCEDURES

This section summarizes the procedures related to the Information Security Policy. The details are written in separate documents. Many of them are in development or testing, and they will be revised frequently as we improve our processes.

The security procedures are tied to Information Classifications of Internal, Open access, Confidential-Organization and Confidential-GDPR – see the Definitions section above.

Most of the security protections are provided through the GDPR-compliant functionality provided by Amazon Web Services (on Canadian servers) and on Microsoft Office 365 collaboration tools (most of which are on Canadian servers). Third-party audit reports of those protections can be found in the SIS Security White Paper (see link above).

Personal information classified as Confidential-GDPR will be protected from warrants and subpoenas from foreign governments through encryption that is managed by LogicalOutcomes using decryption keys that are not accessible to Amazon Web Services or Microsoft.

7.1 DEFINE ROLES FOR EACH PROJECT (RESPONSIBILITY OF EXECUTIVE DIRECTOR AND PROJECT MANAGER)

Each project, including internal projects like financial management and human resources activities, will be assigned a Project Manager and team members. See the Responsibilities section above.

7.2 SET UP PROJECT TEAMS (RESPONSIBILITY OF PROJECT MANAGER)

a. Assess privacy risk and label projects and folders

- ☐ Fill out the Privacy Risk Assessment form[5].
- ☐ In consultation with the client organization, assign the project's correct confidentiality level within the Project Charter[6] (Open Access or Internal or Confidential-Organization).
- ☐ Identify any Confidential-Organization or Confidential-GDPR materials that must be managed within the project.
- ☐ Based on the assessment, set up the project and folders in Microsoft Teams as described below, or assign an administrative assistant to do so.
- ☐ Save the Privacy Risk Assessment in the Team SharePoint library.

[5] Our privacy risk assessment is adapted from https://digital.nhs.uk/article/8489/Health-and-social-care-data-risk-model-, which may be reused for internal use but not shared publicly.

[6] Similar to a Statement of Work or Terms of Reference

b. For Internal Teams (default)

- ☐ Create a private Microsoft Team with the Project Manager as owner. The Project Manager may assign others as owners. Bots or apps outside Office 365 must be approved by the Project Manager before being added to the Team.
- ☐ Label SharePoint document folders as Confidential-Organization if required (default label is Internal).
- ☐ Allow the use of external information services within Microsoft Teams (e.g., Zoho Desk, WordPress, GitHub) but ensure that no confidential information is used in those services.

c. For Open Access Teams

- ☐ Create a public Microsoft Team that is open to all users with LogicalOutcomes accounts. Any LogicalOutcomes user may invite a guest user to a public Team.
- ☐ Invite guest users to the Team.
- ☐ Allow the use of external applications and services (GitHub etc.)

d. For Confidential Teams

- ☐ Create a private Microsoft Team with one owner, the Project Manager. All members must be approved and added by the Project Manager or, if unavailable, the Executive Director or Project Sponsor. The client organization will be invited to review the project member bios, and to approve new additions to the Microsoft Team.
- ☐ Verify that all project members with access to Confidential information are appropriately trained and qualified.
- ☐ Require multi-factor authentication on any account accessing Confidential information (in the administration settings).
- ☐ Create at least one folder in the Team SharePoint library as Confidential-Organization. (enhanced encryption and access permissions will be applied automatically).
- ☐ Set up the SharePoint library attached to the Team. The project may need multiple protected folders with different people accessing them. If required, folders may also be protected by Cryptomator vaults, but this removes files from Office 365 indexing and makes the information less accessible to team members.
- ☐ If a team member needs access to DHIS2 or LimeSurvey databases with personal information, request the Executive Director or Security Officer to set them up with a user account to a virtual workspace.
- ☐ If passwords to Confidential information must be shared (e.g., for encrypted SharePoint lists and Cryptomator vaults), share them through LastPass without revealing their content.

7.3 Set up policies for project information (responsibility of Security Officer)

- ☐ Create protection policies for each Information Classification using SharePoint and Office 365 access permissions, Cryptomator and LastPass, and document them for Project Managers. Set default Classification as 'Internal'.
- ☐ Set policies for contractor/volunteer training and qualifications for access to Confidential information.
- ☐ Set policies for Confidential-Organization folders and SharePoint libraries with Office 365 access restrictions, including multi-factor authentication.
- ☐ Set policies for hosting and management of online databases containing Confidential-GDPR information.
- ☐ Set policies for Confidential-GDPR folders with Cryptomator vaults.
- ☐ Set policies for sensitive SharePoint list fields with client-managed encryption.
- ☐ Set policies for management of shared passwords through LastPass.
- ☐ Set policies for the adoption of any new online services that handle Confidential information.

7.4 Wrap up projects (responsibility of Project Manager)

- ☐ Identify final versions of project deliverables and label them as Records for archiving within SharePoint.
- ☐ Delete any information that external organizations have requested be deleted at the end of the project, and ask team members to do so also.
- ☐ Remove access permissions from any Confidential information that has been protected by Office 365 enhanced encryption, and change the passwords of Cryptomator vaults.
- ☐ Tidy up the OneNote Notebook and documents within the Team SharePoint document library. If appropriate, copy documents to another Team.
- ☐ Encourage the dissemination of open access materials:
    - ☐ Ask team members to nominate anything they want to share or reuse themselves in the future.
    - ☐ Get written permission from client organization or external co-owners to share open access material, removing identifying information or non-LogicalOutcomes contributions if appropriate.
    - ☐ Zip up the material and post on Zenodo.org, listing all the contributors, both internal and external.
    - ☐ Share the Zenodo DOI with all team members and if appropriate in blog postings.
- ☐ Request the 'Archiving Administrator' to remove all members from the Team, including the Project Manager, and archive the Team documents (requires an E3 or E5 license).

7.5 Obtain contractor and volunteer agreements (responsibility of Project Manager)

- ☐ Ensure that each LogicalOutcomes contractor or volunteer has signed a confidentiality agreement.
- ☐ Ensure that each LogicalOutcomes contractor or volunteer has signed an agreement to manage LogicalOutcomes information correctly, i.e., saving project information in the correct locations, not copying it without permission, and managing their devices and passwords responsibly.[7]

7.6 Manage incidents (responsibility of Project Manager and Executive Director)

- ☐ Document incidents according to the incident management policy (in development]
- ☐ Escalate to the Executive Director and Board

7.7 Audit and report (Responsibility of Data Protection Officer)

- ☐ Review all procedures to determine their compliance with GDPR using Microsoft Compliance Manager, and create test plans.
- ☐ Every three months, audit all Confidential projects to ensure they have been set up according to the procedures above.
- ☐ Every year, audit three Internal projects, selected according to the test plan (in development).
- ☐ Enter findings into Compliance Manager, including recommendations, and assign to the Executive Director for action.
- ☐ Escalate serious incidents to the Executive Director, Security Officer and Chair of Ethics and Privacy Committee (who is a Director of the Board).

7.8 Respond to security issues (responsibility of Executive Director and Board President)

- ☐ Respond in writing to issues raised in incident or audit reports.
- ☐ Make continuous improvements in security procedures.

[7] Our checklist, which will change as security practices change is based partly on the Cyber Aware initiative of the UK government. The core advice is to install the latest software updates and use a strong, separate password for sensitive information.