ToGGeL
TAP ON GLASS GET EVERYTHING LINKED

Information Services Security Awareness Training Policy

Last Update Status: *Updated November 2024*

1. PURPOSE

The purpose of this policy is to ensure that all ToGGeL employees and affiliates with access to ToGGeL data, are taught Information Security Awareness to gain an understanding of the importance of securing ToGGeL data. ToGGeL seeks to establish a culture that ensures that institutional data is secure. This policy and associated procedures establish the minimum requirements for the Security Awareness and Training controls.

2. SCOPE

This policy applies to all ToGGeL employees, staff, partners and identified affiliates.

3. DEFINITIONS AND AUTHORITY

“Security Awareness Training” is a formal process for educating employees about the internet and computer security. A good security awareness program should educate employees about institutional policies and procedures for working with information technology (IT).

“ToGGeL Affiliate” or “Contractor” is someone officially attached or connected to ToGGeL who is not a client or employee (e.g. contractors, vendors, interns, temporary staffing, volunteers and agents.)

“Personally Identifiable Information (PII)” is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymising anonymous data can be considered PII.

“The Protection of Personal Information Act (POPIA)” is a law that protects the privacy of any personal information.

“Data Owner” is a person responsible for the management and fitness of data elements (also known as critical data elements), both the content and metadata.

“Functional Lead” is a technical lead point person for a department. Responsibilities include coordination of upgrades, delegating access and system issues.

4. POLICY

Educating users and administrators at all levels on the safe and responsible use and handling of information is necessary. It is the obligation of ToGGeL and staff to protect ToGGeL owned and personally owned computers containing or having access to electronic information and records. ToGGeL records exist for the purpose of the business of ToGGeL. To facilitate appropriate information security practices the Information Security Office requires specific training based on the classification level of data people have access to.

Full-time staff are required to attend security awareness training upon employment with ToGGeL. The staff or Agent has 60 days to complete the training program, or they will be deemed non-compliant with this policy. Staff with access to PII, as well as data stewards, and functional leads must take security awareness training on a yearly basis. Presently staff are encouraged, but not required, to attend annual security awareness training. All temporary employees who have access to PII information must undergo security awareness training before they can access ToGGeL records. Staff who have not completed the security awareness training will be locked out of the ToGGeL system.

The security awareness training program is subject to yearly review and enhancement based on changes to the information security environment.

5. POLICY COMPLIANCE

5.1 Compliance Measurement

The Information Security Office in conjunction with the IT Service Desk will verify compliance to this policy through various methods including, but not limited to, application tools reports, internal and external audits, and feedback to the Information Security Office.

5.2 Exceptions

Staff members that do not have access to computers or access to PII data. Any other exceptions to this policy must be approved by the Information Security Office in advance or the CIO.

5.3 Non-Compliance

Staff who do not comply with this policy will have network access rights suspended until they comply with the policy.

5.4 Related Policies & Documents

- Data Governance Policy
- Data Classification Policy

5.5 Security Incident

ToGGeL employees that incur security risk exposure (live or simulated) may be required to retake Security Awareness training.

6. REVISION HISTORY

Date of Change	Responsible	Summary of Change
October 2022	ToGGeL CIO	Updated and converted to new format.