Procedure - Third-Party Relationships

Purpose
The purpose of this procedure is to ensure that data security is maintained with third parties that includes an agreed-upon level of security.

Identification of Risks from Third Party Access
The Information Security Officer (ISO) will control authorization for types of access to information processing facilities by third parties based upon the reasons for that access.

A risk assessment will be carried out before any third-party access is granted and will consider the reasons for access as well as the necessary controls to be put in place.

Access of third-parties to information processing facilities will be identified in a written agreement; this access includes the scope of access to physical, logical and network assets.

Security Requirements in Third Party Contracts
In coordination with the data owner, the ISO will control authorization for types of access to information processing facilities and ESD information by third-party contractors.

Access by third-party contractors will be specifically agreed upon and documented in a written agreement.

Arrangements involving third-party access to ESD information processing facilities should be based on formal written agreement containing, or referring to, all the security requirements to ensure compliance with ESD's security policies, procedures, and operating practices. The written agreement should ensure that there is no misunderstanding between the ESD and the third party. ESD should satisfy themselves as to the indemnity of their third-party. The following terms should be considered for inclusion in the written agreement:

- The general policy on information security;
- Asset protection, including:
    - Procedures to protect organizational assets, including information and software;
    - Procedures to determine whether any compromise of the assets, i.e., loss or modification of data, has occurred;
    - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
    - Integrity and availability;
    - Restrictions on copying and disclosing information;
- A description of each service to be made available;
- The target level of service and unacceptable levels of service;
- Provisions for the transfer of staff where appropriate;

- The respective liabilities of the parties to the agreement;
- Responsibilities with respect to legal matters;
- Access control agreements, covering:
    - Permitted access methods, and the control and use of unique identifiers such as user ID's and passwords;
    - An authorization process for user access and privileges;
    - A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with regard to such use;
- The definition of verifiable performance criteria, their monitoring and reporting;
- The right to monitor, and revoke, user activity;
- The right to audit contractual responsibilities or to have those audits carried out by a third party;
- The establishment of an escalation process for problem resolution, contingency arrangements should also be considered where appropriate;
- Responsibilities regarding hardware and software installation and maintenance;
- A clear reporting structure and agreed reporting format;
- A clear and specified process of change management;
- Any required physical protection controls and mechanisms to ensure those controls are followed;
- User and administrator training in methods, procedures and security; · Controls to ensure protection against malicious software (see 8.3)
- Arrangements for reporting, notification and investigation of security incidents and security breaches;
- Involvement of third party with subcontractors.

These security requirements must address the confidentiality of ESD's data.

Software-as-a-Service Third Party Providers
The security requirements of ESD outsourcing the management and control of all or some of its information systems, networks and/or desktop environments should be addressed in a written agreement agreed between the parties.

The written agreement should address:

- How the legal requirements are to be met, i.e., data protection and privacy legislation;
- What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities;
- How the integrity and confidentiality of ESD's business assets are to be maintained and tested;
- What physical and logical controls will be used to restrict and limit the access to the organization's sensitive business information to authorized users;
- How the availability of services is to be maintained in the event of a disaster;
- What levels of physical security are to be provided for outsourced equipment;
- The right of audit

Timeline for Implementation of Procedure

Given the required changes to ESD processes to fully implement this procedure, new technology systems will be subject to this procedure immediately while existing processes or systems will be reviewed as required by the procedure's periodic review. If an operating practice is needed from IT as part of the procedure, IT will develop and have implemented that process before running proposed technology system through it. Procedure to be fully implemented by September 1, 2024.