ACENET Data Security Policy

Introduction

ACENET is committed to protecting the confidentiality, integrity, and availability of data managed by ACENET. Data managed by ACENET refers to data owned by clients and data owned by ACENET.

All data managed by ACENET must be protected in a manner that is considered reasonable and appropriate to their life cycle and sensitivity, as approved by ACENET management. Data owned by ACENET is protected by ACENET internal security policies; data owned by clients is protected from unauthorized access, malicious attacks and exploitation by this policy, in a manner consistent with ACENET's Cybersecurity Policy.

Data privacy and data rights management is beyond the scope of this policy.

Roles and responsibilities

Data Owner

The data owner is the organization or person that has collected or created the data with rights and responsibilities for that data.

ACENET considers client data stored on its systems to be owned by the Account Owner in the Compute Canada Database (CCDB), however in the event of dispute, we will follow the relevant policies of the institution employing the Account Sponsor.

If an Account Sponsor wishes ACENET to provide access to data stored under the account of a user they sponsor, our process will be: 1. Attempt to contact the user storing the data to obtain permission for ACENET adjusting file permissions to include the Account Sponsor. 2. Should step 1 not be successful, ACENET will seek this permission instead from the institution employing the Account Sponsor.

Data Custodian

A data custodian is responsible for maintaining data on the IT infrastructure in accordance with business requirements. ACENET provides and manages infrastructure services for client data. Unless by an agreement with the data owner, ACENET does not fulfil data custodian duties.

Data User

A data user is a user who has been granted access to the data as part of their assigned responsibilities. A data user must follow ACENET cybersecurity policy to access and use data.

Data-in-transition and data-in-use are protected

Data uploaded to ACENET is encrypted during transit.

Data-in-use is defined as information that is being created, deleted, read and written on random access, high-speed primary storage systems. Data stored on primary storage in expired accounts is subject to deletion after a grace period of 4 months from the time of account expiry in the Compute Canada Database (CCDB).

Data-in-use security requires consideration of other ACENET operational security controls. ACENET provides the system security controls, monitors, and audits the process of usage. Data owners should restrict permissions for modifying and processing their data. User access should be limited to the functions required in order to perform assigned tasks.

In addition to the provided security controls (e.g. encryption), data sharing restrictions are based on jurisdiction, in accordance with regulatory requirements.

Data backup is protected

ACENET performs backup of data-in-use to tape media on a daily and weekly schedule to assure disaster recovery. Further requirements of data backup and data archive are based on mutual explicit agreements.

Weekly copies of tape backups are stored in a physically secure location. Access to backup data is restricted to authorized users only. Inactive daily backup versions of dynamic data will be retained for 30 days; the most recent backup version of static data will be retained indefinitely. Once removed from primary storage, the last backup version will be retained for 30 days.

Secure protection for categorized or classified data

For specially categorized or classified data, such as highly sensitive data or that which requires regulatory compliance, ACENET requires an explicit agreement.

Indemnity

While ACENET observes best practices to protect our client data, the data owner is ultimately responsible. ACENET maintains no financial responsibility for data loss on its systems arising from any cause, including but not limited to hardware failure, software malfunction, datacenter issue, accidental deletion, or malicious action.