IT Policy For System Administrators and Managers

Policy/Document Approval Body:	Governance Board
Date Created:	8 March 2020
Policy Custodian:	Deputy Dean
Policy Contact:	IT Manager
File Location:	W:\Data - ALL.Standard\Policies and Procedures\EIT Policies and Procedures
Location on EIT website:	http://www.eit.edu.au/organisation-policies
Definitions (if required):	
Review Period:	Three years from commencement
Revision No:	1
Date of Revision:	
Date Approved:	18 November 2020
Date Commenced:	7 December 2020

1.0 Purpose

This policy establishes requirements and provides guidance to EIT System Administrators and Managers for the ethical and acceptable use of their administrative/elevated access, as well as their duties as administrators/managers.

System Administrators manage, maintain, and monitor EIT's ICT systems, facilities and resources. Managers have the authority to view, add, update and remove sensitive data (which includes personal information of students and staff, medical records, payment details, company track records etc.). Both parties have the responsibility of ensuring the right personnel have access to the relevant information and to not breach the security and integrity of the system they are assigned to.

2.0 Scope

This policy applies to all ICT systems, facilities and resources owned or operated by or on behalf of EIT. All EIT managers and system administrators (including external third parties engaged under a contract) with access to EIT's resources and have the ability to update files and folder access permissions are responsible for adhering to this policy.

3.0 Policy

Each administrator or manager's elevated access privileges have to be evaluated and given access to only relevant data, materials and/or staff and student files.

When their job responsibilities change, the access privileges have to be reviewed and updated accordingly.

4.0 Permitted Activities

4.1 Operational Activities

To ensure smooth operation of the network and ICT systems, the relevant administrators may:

- Monitor, manage and report traffic on the networks.
- Examine any resources on the ICT systems.
- Rename or update the permissions on any resources.
- Create new files and resources on the ICT systems.

If a file or resource has been encrypted or password-protected by a user, a system administrator must seek authorization from management or owner of the file before any attempt is made to read the contents.

Any activities undertaken by the administrator must not result in unintentional loss or destruction of information. Approval from the owner or manager of relevant files/resources must be sought prior to deletion/updates.

4.2 Policy Activities

Prior to resorting to the monitoring of user activities, users must be informed and be referred to the policies which will be applied. This can be done either through a general notice to all users, or to individual parties. Once the user(s) has/have been formally notified, the administrator(s) can proceed to:

- Monitor, manage and report traffic on the networks.
- Examine any resources on the ICT systems.
- Rename or update the permissions on any resources.
  Create new files and resources on the ICT systems.

5.0 General Roles and Responsibilities

System administrators oversee all ICT network and systems. A network topology map encompassing all active equipment should be kept up-to-date, and all the devices should be constantly monitored for faults, as well as schedule timely maintenances. Key equipment should be manageable remotely in case of time-sensitive troubleshooting is required.

To minimize the risk of cyber-attacks and intrusions, system administrators should protect the ICT network accordingly by:

- Restricting (physical/remote) access to key devices.
- Enabling multi-factor authentication on all user accounts, especially administrator accounts.
- Using highly complex passwords and authenticator apps for user logins.
- Implementing ACLs (IP address and/or user accounts) wherever possible, especially on servers and key devices.
- Keeping logs of failed login attempts/errors/audit failures for key devices, and get notified of abnormal behaviours.
- Protecting logs from any unauthorised access or modification, and synchronise system clocks via the ntp to ensure accurate timestamping of the log events.
- Enforcing strong remote encryption when accessing key devices, such as SSH.

A user with elevated access (administrators and managers) privilege must:

- Never use their access status to satisfy personal curiosity about an individual, system, practice or contracts.

- Never share their personal login details.
- Ensure that the elevated access is consistent with an individual's roles and responsibilities.
- In fulfilling the responsibilities that accompany the granting of Elevated Access, take all reasonable measures to protect the confidentiality, integrity, and availability of Information Resources.
- Take steps to ensure adherence to and compliance of all hardware and software license agreements.
- Never expose or disclose information obtained through elevated access privilege.
- Not use their access privilege for any purpose outside of the scope for which it was granted make sure their accounts are secured with a complex password, and is changed at least every 60 days.

System administrators are also expected to:

- Delete or disabled old/unused user accounts.
- Make sure they have a disaster recovery plans for all key devices.
- Perform regular system backups.
- Test backups and recovery procedures periodically.
- Keep at least 2 generations of backup for each system.
- Handle backups confidentially since they contain sensitive data.
- Take 1 copy of backups off-site to prevent any damage from a disaster at the main data site.

6.0 Management responsibility

- Management should make the decisions on permissions for specific resources and overall network access.
- The action of permissions delegation is a big responsibility, therefore individuals with this authority should be carefully vetted and must demonstrate good integrity.
- The onus is on the managers to ensure that the infrastructure administrators are capable in facilitating these sensitive tasks.
- The onus is on the administrators to understand the IT policies and procedures in detail, ensuring various activities do not contravene the stipulations of these documents.
- Management must understand the importance and oversee the administration activities; both the help desk and maintenance aspects.

7.0 Ethical considerations

System administrators and managers will inevitably come into contact with sensitive, personal or restricted information during the course of their duties. For these reasons they must display an exemplary work ethic. Any information obtained must be treated as confidential - it must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific incident handling procedure:

- Sensitive information pertaining to an incident must be restricted to only the appropriate management roles. Any unrelated information to the incident must not be disclosed.
- The only exception to this requirement is if information is requested by a relevant government department.

Data security is a critical component of an administrator's job. Anyone in this role must be capable of understanding the various levels of data sensitivity, and categorization of data across the organization. Appropriate disclosure of data to relevant stakeholders is also critical to the role.

Professionalism within an administrator role is expected, as the scope of the role is all-encompassing; working with all stakeholders internal and external to the organization. Encouraging or engaging in activities that may impede the integrity and security of the organisation's infrastructure is improper conduct; these types of activities could consist of:

- Malicious vandalism or distribution of EIT/IDC records.
- Malicious intent to access materials that an individual is not authorised to read.
- Provide individuals with elevated privileges and access in return for favours.
- Manipulate software or hardware maliciously with the intention of accessing or modifying records.
- Any malicious intent to breach the IT policy.

A core responsibility of administrators is to ensure that stakeholders are appropriately informed about anything that may impact them. Some aspects of the business that may impact them consist of (but not exclusively):

- Security considerations; conducting daily activities in a secure manner.
- Acceptable usage of equipment and data.
- Data backup procedures and disaster recovery approaches.

Due to the privileges held by administrators, conflicts of interest must be declared immediately to managers or any other relevant personnel. Monitoring or collection of stakeholder information must be undertaken in situations only where specifically authorized to do so.

8.0 Definitions

Elevated Access: A level of access that is authorized to perform functions that ordinary users are not authorized to perform

ICT: Information and Communication Technologies

System Administrator: A User with a level of access above that of a normal User, or with supervisory responsibility for Information Systems and Information Resources.

9.0 Related Documents

- ICT Services and Facilities Use Policy
- Privacy Policy
- Records Management Policy

This policy has been written with reference to The University of Glasgow's Guidelines for System and Network Administrators:
https://www.gla.ac.uk/myglasgow/it/informationsecurity/policies/guidelinesforsystemandnetworkadministrators/