



Information Communication Technology (ICT) Information Security Policy





DIRECTORATE: OFFICE OF THE CEO	
SUBJECT: ICT SECURITY POLICY	POLICY NO:
REV NO: 1	REV DATE: 10 May 2023
SUB-DIRECTORATE: Information Management	BOARD ITEM NO:
SIGNATURE:	
DATE APPROVED:	EFFECTIVE DATE: 01 July 2023

1. POLICY STATEMENT

To communicate policy statement that is aimed at ensuring that only authorized users have timely and appropriate access to computerized information, while safeguarding the information's confidentiality, security, and integrity.

Access to CENTLEC's network/ systems/ applications must be restricted to only authorized user or processes based on a need-to-know principle due to duties performed by the user.

Attached policy appendices serves to outline the boundaries and procedures for the CENTLEC ICT work force and user community and official documentation to complete.

2. OBJECTIVE

The objective of this policy is to ensure the Institution has adequate controls to restrict access to systems and data.

The policy shall further provide mechanisms to secure information against loss, destruction, tampering, and unauthorized access or use.

3. SCOPE

All CENTLEC employees, trainees, consultants, contractors, agents must be authorized in accessing the organisations network, IT systems and applications.

To secure all IT systems or applications managed by CENTLEC or its service providers that process, store or transmit information including network and computer hardware, software and applications, mobile devices, and telecommunication system must comply with the security policy for access and authorization.

4. ABBREVIATIONS

- | | | |
|-----|-----|--|
| 4.1 | IDS | - Intrusion detection system |
| 4.2 | IPS | - Intrusion prevention systems |
| 4.3 | ICT | - Information Communication Technology |
| 4.4 | USB | - Universal serial bus |
| 4.5 | ISO | - Information Security Officer |
| 4.6 | APN | - Access point name |

- 4.7 VPN - Virtual private network

5. RELATED DOCUMENTS

This policy is relate to user access policy, physical and environmental control, firewall policy, internet policy, change control policy, Incident Management Plan, and identity management policy.

6. DEFINITIONS

- 6.1 **Firewall** - is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- 6.2 **Intrusion detection system** - is a device or software application that monitors a network or systems for malicious activity or policy violations.
- 6.3 **Intrusion Prevention System** is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
- 6.4 **Universal Serial Bus** is a set of connectivity specifications developed in collaboration with industry leaders.
- 6.5 **Password** is a string of characters used to verify the identity of a user during the authentication process.
- 6.6 **Digital certificates** are electronic credentials that bind the identity of the certificate owner to a pair of electronic encryption keys, (one public and one private), that can be used to encrypt and sign information digitally.
- 6.7 **Endpoint device** is a LAN- or WAN-connected hardware device that communicates across a network.
- 6.8 **Access point name (APN)** is the name of a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network, frequently the public Internet.
- 6.9 **Virtual private network** extends a private network across a public network and enables users to send and receive data across shared or

public networks as if their computing devices were directly connected to the private network.

7. NETWORK SECURITY

Traffic between the organizational network and the Internet controlled for:

- 7.1 Unauthorized access on service applications and ports using firewall devices must be established.
- 7.2 Control of potential attacks, using an intrusion detection or prevention method (IDS/IPS) to prevent unauthorized access to the network.
- 7.3 Preventions of malicious code, spam and suspicious traffic, using an anti-malware to inspect malware in emails and other open ports on Critical and sensitive application servers, databases and services must not be directly accessible from the Internet

8. MONITORING AND NOTIFICATIONS

- 8.1 **Systems**
Any change effected on the system relating to operating systems, databases and applications should notify the administrator group using any form of communication for monitoring.
- 8.2 **Network**
24/7 intrusion-detection monitoring will be conducted by using intrusion-detection tools and keep audit logs for the system servers, software, database, networks, and firewalls. Administrators submit reports on daily for assessment and possible corrective action for immediate corrective action will be taken to help eliminate system vulnerabilities or to prevent future intrusion attempts. Immediate notification management via a predefined emergency notification list should notify manager for the affected network. Wherein intrusions are suspected or confirmed by the user, the user shall follow the ICT Incident management plan for reporting the incident.

9. ANTI-MALWARE

Detection, prevention, and recovery controls to protect against malicious code, along with appropriate user awareness procedures must be implemented in all CENTLEC endpoints. Anti-malware software must be configured to enable real-time scanning and inspection of all incoming or outgoing emails. Endpoint devices and servers that cannot be managed by the central anti-malware or end-point protection management console must be equipped with an alternative anti-malware solution.

10. ACCESS TO ICT RESOURCES

Only persons who have valid business reasons or approvals for accessing the CENTLEC information resources will be granted access. Individuals will be given access to information resources as per signed approval forms.

No one may access CENTLEC information resources or applications without prior written authorization and approval from the Head of ICT. Authorization and approval must be obtained using the appropriate access request forms. It is illegal to use any computer or access information stored or maintained by ICT without the proper authorization and consent of the ICT department.

The new employee or existing employee requiring access to CENTLEC resources must provide a relevant completed access request form with all the - employee details including the level of the required access.

The access request form must be authorized and approved at appropriate directorate levels for remote users (e.g., employees, contractors, third parties) with access to critical systems.

Personal information saved on the CENTLEC assets would be wipe and not be recovered during the assets maintenance or repair. All users are urged to save CENTLEC data on the provided shared drives; information not saved on the shared drive guided by ICT would not be recovered. It is the responsibility of the users to save data on shared drive provided by ICT.

Anyone who signs on to a computer system must sign off and/or physically secure the terminal or PC when leaving it unattended. Where possible, computer systems

will be set up to automatically sign off after 10-15 minutes or password-protect terminals.

Access to computer center / server room will be secure by means of locked entryways. Only persons who is authorized to operate or maintain the computer systems will be issue access cards, or other means for unlocking the entryway.

11. PRIVILEGE ACCOUNTS

A nominative and individual privileged user account must be created for administrator accounts, instead of generic administrator account names. Such an account should be assigned to an individual using a description such as "first_name, last_name, admin" Managers or supervisors can only request privileged user accounts or an employee nominated by the manager and must be appropriately approved. Password for admin account should be changed every 30 days. This includes general user accounts such as "guest" and "functional" accounts. Administrator must review access and privilege provided in the log files.

12. SHARED USER ACCOUNTS

The use of shared accounts is prohibited unless otherwise required for business reasons. Written approval must be obtained to provide the rational for shared accounts. Where possible, the use of specific network domain "security groups" should be used to share common access permissions across many users, instead of shared accounts.

Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as "guest" and "functional" accounts. Administrator must review access and privilege provided in the log files.

13. SECURITY AWARENESS

Administrators managing user access must perform security awareness to ensure that user understand security around ICT. This security awareness can be in the form of email communication, workshops, flyers, billboards, presentations, and computer popups. ICT must enforce the effectiveness of this on a quarterly basis,

preferability monthly followed by workshops. It is the responsibility of each user to ensure that they practice security awareness communicated to protect the environment. Administrators are compiled to be aware of any changes happened on the environment. This type of alert can be information of email, SMS, change logs or screenshot. All the changes to the network environment or servers, devices, or databases. Changes took place in the environment must be keep safe by the administrators. Network diagram must have the latest updates of the changes made.

14. USE OF ICT EQUIPMENT

CENTLEC computer equipment may only be utilised for performing business functions. The use of computer equipment for non-business-related matters forbidden. No private files or folders of any nature may be stored on the CENTLEC computer equipment. No authorized persons will secure terminals, network devices, and personal computers in unsecured areas against theft and use. Personal use of this equipment is prohibited. Any data not belonging to CENTLEC will not form part of the data transfer to backup. Such data including the media will be removed from the CENTLEC devices.

15. ACCESS TO SERVER FACILITY

The ICT department will establish a security authorization schedule access to the server room. A visitor's logbook is kept and signed by all personnel that visit the secure area. The authorized CENTLEC or ICT staff, who will accept full responsibility while the visitor is inside any secure area, will escort authorized visitors to the ICT server rooms, computer rooms and or ICT department offices. Equipment in the server room should be monitored by means of digital cameras. Biometric access must be installed with the server records for the access.

16. SECURITY OF COMPUTER-RELATED MEDIA

Confidential and sensitive business-related information would not be left on desks or exposed to anyone for accessibility. All external drives containing CENTLEC data should be locked and not be accessible by unauthorized personnel.

Auto-run of content from removable media should be disabled for any espionage

Devices with access to sensitive information should be identified and require additional access control to access this information. Removable media access to CENTLEC assets must be controlled using software tools to block or monitor the access.

17. PROTECTION OF COMPUTERISED FILES

Antivirus protection programs will be installed and executed regularly on all computers and servers. Software will not be copied from public access internet or other non-CENTLEC computer systems without first being scanned using a virus protection program. All employees will use only licensed software and authorized by CENTLEC. All other third-party software, which are not authorized by CENTLEC ICT, should be wiped off from CENTLEC computers.

The storage or use of unlicensed software is not allowed. Passwords encryption will be used where disks, directories, files, and other computer resources are shared between users. USB Access prohibited on the CENTLEC assets; accept on the certain cases, which need to be authorized. Data encryption mechanism must be used to encrypt to prevent authorized access to stolen or lost devices.

18. ACCESS TO INFORMATION RESOURCES

The remote connection to facility provided by CENTLEC will only be used for support purposes and work related through authorization and access approval. Authorized employees, contractors, and other authorized parties will be permitted to use remote connections such as APN, VPN, or any secured remote platform to access CENTLEC information resources after work hours, with proper safeguards. Illegal remote espionage or sabotage is not permitted for users or contractors access resources remotely. Remote access be monitored by ICT to ensure compliance for the access provided. Such access should be recorded.

19. ELECTRONIC COMMUNICATION

E-mail is a tool for business communications only, and users have the responsibility to use this resource in an efficient, effective, ethical, and lawful manner. All e-mails created, send, or received on the e-mail systems are the property of CENTLEC.

CENTLEC has the right to assess, monitor and retrieve any e-mail for legitimate business reasons, including without limitation, compliance, or non-compliance with this policy. Emails encryption mechanisms should be implemented to secure end-to-end data communication using certified digital signature certificates.

20. SECURED WEB-BASED INFORMATION

Access to web pages should be controlled according to the level of confidentiality of the information and the risk involving access thereto. The implementation of these access control mechanisms should regularly be checked for possible security flaws and questionable risks.

Digital certificates should be used where knowledge of a user's password through physical means becomes a considerable risk regarding the confidentiality of the information being dealt with. Website and intranet information will be securely extended to all employees by providing a controlled and secured centralised point of access to all web-based information. Certified digital certificate should be for such purpose.

21. DATA ENCRYPTION

Confidential and sensitive documents should be encrypted using a password; the document will only be accessible to both the sender and the recipient. The sender of the document will forward the password to the recipient of the document by SMS. The document will only be accessible to the person with the password. Data recovery and restore should be applicable to recover or remote wipe sensitive data for lost or stolen item. Data encryption software to protect data on the computers and laptop should be applied and implemented.

22. PASSWORDS SECURITY

All access and security codes such as passwords, Personal Identification Numbers ("PINs") and security tokens are considered as confidential information and must be protected and handled accordingly. The password complexity requirement is always enabled on the network domain all CENTLEC systems

This section applies to Microsoft Windows network domain and shared folders, desktops, laptops, tablets, servers, and databases, including for the domain and the local password policies. Application passwords must rely on network domain credentials where possible (Active Directory Password).

Passwords must combine a minimum length and the use of complex characters. Passwords expiry for all systems should be set at 30 days. Enable password history to not permit the users to use the same password.

All passwords to the computer systems must be confidential. It is a violation of this policy to reveal passwords to anyone without written permission from the ICT department. The hard coding of any password is strictly forbidden. This includes using the "save password" option on any software package if the personal computer is not protected as specified above. All facilities housing computer equipment must be physically protected from any potential damage.

23. ROLES AND RESPONSIBILITIES

Management in each business unit will ensure that all ICT policies are addressed at departmental staff meetings. Management in each business unit is responsible for determining what information resources its employees need to access in order to complete their job functions, that is, the granting of access to information resources should be commensurate with the employee job responsibilities. System User Form should detail all the employee information; access to information resources should be commensurate with the employee's job responsibilities.

It is the responsibility of each employee to adhere to this policy and fill all the detail information. Information security should form part of the new employee induction program and the attendance register should attest as confirmation that the new employee is informed and is aware of the content of this document. Administrators should manage access to the system and reviews the logs. CT Manager should approve the forms after access to the systems.


24. CONSEQUENCE MANAGEMENT

CENTLEC labour relations will take disciplinary action against an employee/anyone who has access to ICT resource or network, in which it violates company policy with the engagement of ICT manager.

25. REVIEW AND APPROVAL

This policy and underlying strategies will be reviewed at least annually, or as necessary, to ensure its continued application and relevance.


Revised by:

Signed: 
Manager: Information Management
Date: 22/05/2023

Supported by:

Signed: 
Act Executive Manager: Engineering Retail
Date: 22/05/2023

Approved by:

Signed: 
Chief Executive Officer
Date: 22/05/2023