System access and authorization

- All corporate computers shall be joined to the Active Directory-Domain Controller for proper management and access to institutional resources.
- **Connection to the local area network (LAN):** End-user/Personal computers that have been out of office shall be automatically updated with the latest antivirus.
- **Computers:** users shall terminate active sessions or log out of their computers when moving away from the workstation unless they lock the computer and re-enter the password as required.
- **Computer rooms and storage facilities**: shall always be locked when unattended. Failure to apply necessary protection for equipment shall constitute neglect and the user may be held liable for any loss.
- All users shall be responsible for the safety and custodianship of the end-user devices (laptops, tablets and Smartphones) in the office and outside the office.
- **Standardization of hardware and software:** IT administrators shall standardize computer software and hardware for users based on but not limited to job function, division, and the least privilege principle.
- **Printers and scanners operation:** users shall be required to share printers on the network based on physical proximity and division for resources optimization where applicable. IT administrators shall ensure that all management interfaces of printers are protected by a password to prevent unauthorized use or configuration.
- Individuals shall take care of efficient management of printing resources by only printing when a paper copy is necessary. Sensitive or classified printed documents shall immediately be removed from the printer after printing to prevent unwanted information disclosures. Only authorized maintenance personnel shall carry out printer repairs.
- **Remote administration and security:** This is the ability to manage and monitor systems, servers and network devices from a location other than their physical presence. While remote administration offers convenience and flexibility, it also presents security for security. Therefore, IT Personnel shall be cautious when providing remote support as well as accessing Office resources while at home.
- **License Activations:** Government institutions shall ensure that computers and Servers are installed and activated with genuine Operating systems and license keys.

Revision #2
Created 11 July 2025 15:07:43 by RISA
Updated 14 July 2025 07:34:08 by RISA