Cyber Security

- Minimizing the exposure of systems to external networks
- Implement network segmentation
- Establish role-based access controls and implement system logging
- Implement passwords policy
- Institution level cyber security awareness
- Perform regular vulnerability assessment and penetration testing

Minimizing the exposure of systems to external networks

- nstall and configure gateway firewall, IPsec and SSL VPN, and wireless;
- Configure inbound and outbound Access Control List (ACL) to control only required and legitimate traffic only to be allowed to go in and out of the network;
- Close all the ports and only open the required port;
- Avoid “any” “any” rules set up in all the configurations;
- All rules must be configured to ensure no “ unwanted services” or “hosts” are exposed to the internet, web protection anti-malware, web and app visibility, control, and protection;
- Implement network segregation by having **Demilitarized Zone (DMZ)** for public facing servers, server zone and user zone;
- Ensure that the network is secure by segregating different administrative duties; consider network protection including IPS, REB, HYML5 VPN, ATP, and Security Heartbeat.
- All remote access to ICT infrastructure should be done via VPN.

Implement network segmentation

- **Access control:** should start with IT assets, data, and personnel classification into specific groups, and restrict related access through VLAN.
- **Access management:** access to VLANs should be restricted by isolating them from one another and dispatching resources into different VLANs, so that a compromised system in one segment does not translate into exploitation of the entire network.
- **Use of secure remote access methods:** any remote access to the organization network or system should be secured through VPN for any remote access required. Remote access should be further hardened by limiting the number of IP addresses that are allowed to connect remotely for security and safeness.

Establish role-based access controls and implement system logging

- **Role-based access control:** access to network resources should be granted or denied based on job functions. Permissions should be defined based on the level of access needed to perform job functions and related duties.
- **Standard operating procedures:** should be established to allow the removal from network access of former employees and contractors.
- **Logging capability for each system:** should be implemented for each user and for each activity.

Implement passwords policy

- Strictly use strong passwords with minimum 8 characters comprised of alpha numerical and special characters, as was described in section 6.3;
- Users should have different passwords for different accounts;
- All default passwords must be changed upon installation of new software or new Operating System (OS);
- Failed login attempts should be limited to three times and then lock the user;
- Account lockout duration should be at minimum 20 minutes at maximum 1hour.
- A two-factor authentication should be set up for critical applications and/or systems.

Institution level cyber security awareness

Government institution must plan for and conduct regular internal cyber security awareness for end users at 3 times per year in partnership with RISA.

Perform regular vulnerability assessment and penetration testing

- **Preventive maintenance:** government institutions should plan and perform IT infrastructure vulnerability assessment and penetration testing at least once a year.
- **Incidence response:** government institutions should be prepared to mitigate or to respond as quickly as possible to a cyber-incident, which can hit the organization. A proper disaster recovery plan should also be put in place to insure business continuity while recovering from such an incident.