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.

Revision #1
Created 1 October 2025 10:55:53 by RISA
Updated 1 October 2025 10:57:17 by RISA