# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** |
| --- |
| The three hardening tools that the organization can implement would be<br>1) Encryption using the latest standards<br>2) Firewall maintenance<br>3) Network access privileges<br><br>Methods to implement Encryption would be to make sure that any data sent out is encrypted using the latest and most advanced encryption standard and also to decrypt the data coming from outside into the network.<br><br>Firewall maintenance - Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.<br><br>Network access privileges - It is to permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc. |

| **Part 2: Explain your recommendations** |
| --- |
| **1. Encryption Using the Latest Standards**<br><br>● **Purpose**: Protect sensitive data during transmission and storage by making it unreadable to unauthorized parties.<br>● **Implementation**:<br>○ Ensure all outbound data is encrypted using advanced encryption protocols, such as AES-256 or TLS 1.3.<br>○ Configure the system to automatically decrypt incoming data if it originates from a trusted source.<br>○ Regularly update encryption algorithms to address vulnerabilities in outdated standards. |

## 2. Firewall Maintenance

- **Purpose**: Strengthen perimeter defenses to block unauthorized access and filter malicious traffic.
- **Implementation**:
    - Regularly review and update firewall rules to reflect evolving threats.
    - Use Intrusion Detection and Prevention Systems (IDS/IPS) to enhance the firewall's capability in identifying unusual patterns.
    - Perform routine testing and audits to validate firewall configurations and maintain performance.

## 3. Network Access Privileges

- **Purpose**: Limit access to critical network assets, reducing insider and external threats.
- **Implementation**:
    - Define roles and implement role-based access control (RBAC) to assign minimum necessary permissions.
    - Use IP and MAC address filtering to control device access.
    - Conduct regular audits of access logs and update permissions based on user role changes or security needs.

Together, these measures create a layered security strategy, addressing both internal and external vulnerabilities while enhancing data protection, access control, and system integrity