1. **Enable MFA for all remote access, access to platforms like Microsoft 365.**

2. **Define, maintain and test the following standard operating procedures (SOPs):**
   - Configures a network share as "read-only" for all users and disables guest access.
   - Isolates hosts from the network entirely.
   - Disable user and service accounts and disconnect all sessions from network systems.
   - Block the following on endpoints, servers, and network systems:
     - Domain
     - IP or range of IPs
     - URL pattern
   - Collect and retrieve forensic artifacts at scale.
   - Redeploy and reconfigure all I.T. systems at scale.
   - Configure a network share as "read-only" for all users.

3. **Have the following documents available as hard copies and offsite:**
   - Critical assets list
   - Network diagrams
   - Mobile phone contact lists

4. **Integrate a ransomware attack scenario into your business continuity planning:**
   - Business continuity plan
   - Emergency communication means planned
   - Emergency procedures stored in an alternative location
   - Plan for response when most critical applications are affected
   - Plan for the potential disruption of all critical I.T. systems

5. **Build resilience continuously—prevention is always better than cure:**
   - Enable MFA for all remote access, access to platforms like Microsoft 365.
   - Limit local administrator rights—grant 8-9 only to users who need it.
   - Display Microsoft’s Local Administrator Password Solution (LAPS) to ensure accounts have unique credentials on every device.
   - Run compulsory security awareness training programs.
   - Enable MFA for all remote access, access to platforms like Microsoft 365.

6. **Implement data backup processes:**
   - Regularly backup critical data offsite.
   - Collect and restore forensic artifacts at scale.
   - Test restore processes continually.

7. **Define, maintain and test the following standard operating procedures (SOPs):**
   - Configures a network share as "read-only" for all users and disables guest access.
   - Isolates hosts from the network entirely.
   - Disable user and service accounts and disconnect all sessions from network systems.
   - Block the following on endpoints, servers, and network systems:
     - Domain
     - IP or range of IPs
     - URL pattern
   - Collect and retrieve forensic artifacts at scale.
   - Redeploy and reconfigure all I.T. systems at scale.
   - Configure a network share as "read-only" for all users.

8. **Have the following documents available as hard copies and offsite:**
   - Critical assets list
   - Network diagrams
   - Mobile phone contact lists

9. **Integrate a ransomware attack scenario into your business continuity planning:**
   - Business continuity plan
   - Emergency communication means planned
   - Emergency procedures stored in an alternative location
   - Plan for response when most critical applications are affected
   - Plan for the potential disruption of all critical I.T. systems

10. **Build resilience continuously—prevention is always better than cure:**
    - Enable MFA for all remote access, access to platforms like Microsoft 365.
    - Limit local administrator rights—grant 8-9 only to users who need it.
    - Display Microsoft’s Local Administrator Password Solution (LAPS) to ensure accounts have unique credentials on every device.
    - Run compulsory security awareness training programs.
    - Enable MFA for all remote access, access to platforms like Microsoft 365.