Remote Desktop Protocol (RDP) Security Policy

1. Purpose

The purpose of this policy is to define the requirements for securely implementing and managing Remote Desktop Protocol (RDP) access to protect organizational information systems from unauthorized access, misuse, or compromise.

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who require RDP access to the organizationâ€™s network, servers, or workstations.

3. Policy

- RDP access must be restricted to authorized users only, based on business requirements.
- All RDP connections must be protected by strong authentication methods, including multi-factor authentication (MFA) where applicable.
- RDP access must occur over a secure channel, such as VPN or via gateway services, and never directly exposed to the public internet.
- Network-level authentication (NLA) must be enabled for all RDP sessions.
- All RDP connections must be logged and monitored. Audit logs must be retained according to organizational policy.
- Account lockout policies must be enforced to prevent brute-force attacks.
- Idle RDP sessions must be configured to automatically disconnect after a defined period of inactivity.
- RDP access privileges must be reviewed regularly and removed immediately when no longer required.
- RDP client and server software must be kept up-to-date with the latest security patches.

4. Enforcement

Any employee or affiliate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract, in compliance with organizational HR procedures.

5. Review and Revision

This policy will be reviewed on an annual basis and updated as needed to reflect changes in organizational requirements or security best practices.