|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Standard**:  **Remote Access** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Remote Access Standard is to establish secure and authorized methods for accessing organizational resources and services from remote locations. This is critical in an increasingly digital and mobile work environment where employees, contractors, and third-party vendors need to access sensitive information and systems while outside of traditional office settings. By defining specific protocols for remote access, the policy addresses major security concerns such as unauthorized access, the risk of malware from unprotected devices, and vulnerabilities associated with unsecured networks. It ensures that remote access aligns with best practices, particularly those outlined in the NIST Cybersecurity Framework 2.0, thereby enhancing the organization’s overall cybersecurity posture.

The benefits of the Remote Access Standard are multifaceted. Firstly, it protects sensitive organizational information by establishing stringent access controls and authentication measures, reducing the risk of data breaches. Secondly, it facilitates business continuity by allowing employees to perform their duties securely from various locations, thereby promoting flexibility and productivity. Additionally, by outlining approved methods of remote access and requiring compliance with security protocols, the policy helps to mitigate potential threats associated with remote work, such as the use of infected devices and unauthorized connections. Finally, the policy reinforces accountability by clearly defining the responsibilities of all users, which not only helps in safeguarding the organization's assets but also ensures that all personnel are aware of and adhere to necessary security measures, thereby fostering a culture of security awareness across the organization.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

Remote access is allowed when there is a clear, documented business need. Access may be allowed from entity-issued or personally-owned devices, at the discretion of the entity and in accordance with the standards below. Such access must be limited to only those systems necessary for needed functions.

* 1. Approved Methods of Remote Access

Approved methods of remote access to systems are listed in order of preference.

1. Portals - a server that offers access to one or more applications through a single centralized interface that provides authentication (e.g., web-based portal, virtual desktop interface (VDI)).
2. Direct Application Access – accessing an application directly with the application providing its own security (e.g., webmail, https).
3. Remote System Control – controlling a system remotely from a location other than the entity’s internal network.
4. Tunneling - a secure communication channel through which information can be transmitted between networks (e.g., Virtual Private Network (VPN)).
   1. Required Controls
5. Any method of remote access must use a centrally managed authentication system for administration and user access.
6. Devices and software used for remote access must be approved after review by the Information Security officer/designated security representative. Blanket approvals may be provided based on this review.
7. The authentication token used for remote access must conform to the requirements of the appropriate assurance level.
8. Remote access sessions must require re-authentication after 30 minutes of inactivity.
9. Remote access sessions must not last any longer than 24 hours.
10. The entity must monitor for unauthorized remote connections and other anomalous activity and take appropriate incident response action as per the Cyber Incident Response Standard.
11. Tunneling specific controls:
    1. No split tunneling is allowed.
    2. Network controls regulating access to the remote access endpoint and between remote devices and networks are required.
    3. When a remote access device will have access to other networked devices on the internal network, the remote device must be authenticated such that configuration of the device is compliant with applicable policies.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security](https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final)

[National Institute of Standards and Technology (NIST) Special Publication 800-113, Guide to SSL VPNs](https://csrc.nist.gov/publications/detail/sp/800-113/final)

[National Institute of Standards and Technology (NIST) Special Publication 800-114, User's Guide to Securing External Devices for Telework and Remote Access](https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final)