|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **Remote Access** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 1.0 Purpose and Benefits

The purpose of this standard is to establish authorized methods for remotely accessing resources and services securely.

Major security concerns with remote access include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external hosts, potential damage to resources, and unauthorized access to information.

# 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 [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.

# 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)).

### Required Controls

1. Any method of remote access must use a centrally managed authentication system for administration and user access.
2. 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.
3. The authentication token used for remote access must conform to the requirements of the appropriate assurance level.
4. Remote access sessions must require re-authentication after 30 minutes of inactivity.
5. Remote access sessions must not last any longer than 24 hours.
6. 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.
7. 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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Review and Revisions

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)

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

[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)