| [Insert Company Name and Logo] | |
|---|---|
| **Title: Remote Access Policy** | **P&P #:** |
| **Approval Date:** | **Review:** |
| **Effective Date:** | **Security Team** |

**Purpose**: This policy establishes uniform security requirements for all authorized users who require remote electronic access to [Insert Company name] network and information assets. The guidelines set forth in this policy are designed to minimize unauthorized use of [Insert Company name]'s resources and confidential information.

**Scope:** This policy applies to all users who work outside of the organization's internal network environment, who connect to the organization's network systems, applications, and data from a remote location, including but not limited to applications that contain sensitive and/or regulated data. Users may include members of the workforce, business associates, and vendors. These users may have permanent or temporary access, which may include temporary emergency remote access.

**Definitions:**

1. Defined Network Perimeter: Refers to the boundaries of the [Insert Company name] internal computer network.
2. Sensitive and/or regulated data: Data that includes information regulated by governing agencies, such as Protected Health information (PHI.)
3. Firewalls: A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A firewall is a set of hardware and/or related programs providing protection from attacks, probes, scans, and unauthorized access by separating the internal network from the Internet.
4. Information Resources: Networks, systems, applications, and data including but not limited to, sensitive and regulated data received, created, maintained, or transmitted by the [Insert Company name].
5. Privileged Access Controls: Includes unique user IDs and user privilege restriction mechanisms such as directory and file access permission, and role-based access control mechanisms.
6. Remote Access: The ability to gain access to [Insert Company name] network from outside the network perimeter. Common methods of communication from the remote computer to [Insert Company name] network includes, but is not limited to, Virtual Private Networks (VPN), web-based Secure Socket Layer (SSL) portals, and other methods which employ encrypted communication technologies.
7. Role-Based Access: Access control mechanisms based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on the least-privilege principle.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

8. Web-based Portal:  A secure website offering access to applications and/or data without establishing a direct connection between the computer and the hosting system. Web-based portals most often use 128-bit or higher SSL encryption.
9. Workforce Member: Employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether they are paid by the covered entity.

**Procedure:**

1. Gaining Remote Access
    a. Workforce members will apply for remote access connections by completing a “System Access Request” form. Remote Access is strictly controlled and made available only to workforce members with a defined business need, at the discretion of the workforce member’s manager, and with approval by the Security Officer or designee.
    b. Business associates, contractors, and vendors may be granted remote access to the network, provided they have a contract or agreement with [Insert Company name] that clearly defines the type of remote access permitted (i.e., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the Security Officer and/or legal department before remote access will be permitted. Remote access is strictly controlled and made available only to business associates and vendors with a defined business need, at the discretion of and approval by the Security Officer or designee.
    c. The workforce member is responsible for adhering to all [Insert Company name] policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for [Insert Company name].
    d. All users granted remote access privileges must sign and comply with the “Remote Access User Agreement” kept on file with the Human Resources Department or other department as determined by the [Insert Company name].
    e. It is the user’s responsibility to ensure that the remote worksite meets security and configuration standards established by [Insert Company name]. This includes configuration of personal routers and wireless networks.

2. Equipment, Software, and Hardware
    a. The organization will provide all equipment or supplies necessary to ensure proper protection of information to which the user has access.  The following assists in defining the equipment and environment required (optional).
        i. Organization Provided:
            1. Encrypted workstation
            2. Cable lock to secure the workstation to a fixed object

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

            3. If using a VPN, an organization issued hardware firewall
            4. If printing, an organization supplied printer
            5. If approved by the organization’s Security Officer, an organization supplied phone
        ii. User Provided:
            1. Broadband connection and fees
            2. Paper shredder, if applicable.
            3. Secure office environment isolated from visitors and family
            4. A lockable file cabinet or safe to secure documents when unattended
    b. Remote users will be allowed access through use of equipment owned by or leased to the [Insert Company name], or through the use of the workforce member’s personal computer system provided it meets the minimum standards developed by [Insert Company name], as indicated above. [Your organization must determine minimum standards based on FIPS 140-2 or its successor.]
    c. Remote users utilizing personal equipment, software, and hardware are:
        i. Responsible for remote access. [Insert Company name] will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss.
        ii. Responsible for remote access used to connect to the network and meeting [Insert Company name] requirements for remote access. [Insert appropriate detail for remote access requirements.]
        iii. Responsible for the purchase, setup, maintainance or support of any equipment not owned by or leased to [Insert Company name].
    d. Continued service and support of [Insert Company name] owned equipment is completed by Information Technology workforce members. [Insert appropriate detail for remote access requirements]. Troubleshooting of telephone or broadband circuits installed is the primary responsibility of the remote access user and their Internet Service Provider. It is not the responsibility of [Insert Company name] to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by [Insert Company name].
    e. The ability to print a document to a remote printer is not supported without the organization’s approval. Documents that contain confidential business or sensitive or regulated data shall be managed in accordance with the [Insert Company name] confidentiality and information security practices.

3. Security and Privacy
    a. Only authorized remote access users are permitted remote access to any of [Insert Company name] computer systems, computer networks, and/or information, and must adhere to all of [Insert Company name] policies.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

b. It is the responsibility of [Insert Company name] workforce members with remote access privileges to the network to ensure that their remote access connection complies with the same security requirements as the user's on-site connection. Solutions for remote access to devices on the network must comply with established policies.

c. Secure remote access must be strictly controlled through strong authentication in accordance with the Password Policy.

d. At no time should any user of [Insert Company name] network resources provide their login credentials, multi-factor authentication keys or email password to anyone, not even family members. When using a shared personal computer, for example, users should employ encryption and setup separate accounts so that other users of the computer cannot access sensitive data.

e. It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect from [Insert Company name]'s network when access is no longer needed to perform job responsibilities.

f. Remote users shall lock the workstation and/or system(s) when unattended, so that no other individual is able to access any ePHI or organizationally sensitive information.

g. Remote access users are automatically disconnected from the [Insert Company name] network when there is no recognized activity for 20 minutes.

h. It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their username or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.

i. The Remote Access User must report to the Security Officer within 24 hours of any use or disclosure of sensitive or regulated data in a manner not permitted by this Policy or the Agreement.  After the verbal report, the Remote Access User must send a written report to the Security Officer within 72 hours. The report must contain:

    i. The identification of ever remote user including contact information.

    ii. A brief description of what happened, including the date of the unauthorized use or disclosure and the date of the discovery of the unauthorized use or disclosure, if known.

    iii. A description of the types of data involved (such as name, Social Security number, date of birth, home address, or account number).

    iv. A brief description of what the Remote Access User is doing or has done to investigate the unauthorized use or disclosure, mitigate losses to individuals, and protect against any further breaches.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

    v. Identification of the names and respective titles of those who conducted the investigation on behalf of the Remote Access User.

j. The Remote Access User must report to the Security Officer within 24 hours of any security incident of which it becomes aware.

k. Any employee who becomes aware of an unauthorized use or disclosure by a Remote Access User must immediately contact the Security Officer.

l. Remote access users must take necessary precautions to secure all [Insert Company name] equipment and proprietary information in their possession.

m. Virus Protection software is installed on all [Insert Company name] computers and is set to update the virus pattern daily. This update is critical to the security of all data, and must be allowed to complete, i.e., remote users may not stop the update process for Virus Protection on the organization's or the remote user's workstation.

n. A firewall shall be used and may not be disabled for any reason.

o. Copying of confidential information, including sensitive or regulated data, to personal media (hard drive, USB, cd, etc.) is strictly prohibited, unless the organization has granted prior approval in writing.

p. Since online cloud services (e.g., Carbonite, Dropbox, iCloud, Mozy) may allow for data to be copied from an approved network to a network not controlled by [Insert Company name], they are not acceptable for use. Users must consult with IT or the Security Officer for remote file storage mechanisms.

q. [Insert Company name] maintains logs of all activities performed by remote access users while connected to [Insert Company name] network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Accounts that have shown no activity for 30 days will be disabled.

r. Electronic Data Security

    i. Backup procedures have been established that encrypt data moved to an external media. If there is not a backup procedure established, or if [Insert Company name] has external media that is not encrypted, contact the IS Department or Security Officer for assistance.

    ii. Transferring data to the [Insert Company name] requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Users may not circumvent established procedures when transmitting data to the [Insert Company name].

    iii. Users may not send any sensitive or regulated data via e-mail unless it is encrypted. If sensitive or regulated data needs to be transmitted through email, IS or the Security Officer must be contacted to ensure an approved encryption mechanism is used.

s. Paper document security

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

    i. Remote users are prohibited from using or printing paper documents that contain sensitive and/or regulated data.
    ii. Documents containing sensitive or regulated data must be shredded before disposal.

4. Enforcement
    a. Remote access users who violate this policy are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract. Termination of access by remote users is processed in accordance with [Insert Company name] termination policy.
    b. Remote access violations by Business Associates and vendors may result in termination of their agreement, denial of access to the [Insert Company name] network and held liable for any damage to property and equipment.

**Attachments:** None

**Related Policies:** None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.