CITY OF PROVIDENCE

5.3 REMOTE ACCESS VIRTUAL PRIVATE NETWORK (VPN) SECURITY POLICY

Purpose

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the City of Providence network. This policy ensures the confidentiality, integrity, and availability of the City's data and IT infrastructure, minimizing the risk of unauthorized access, data breaches, and other security threats.

Scope

This policy applies to all City of Providence employees, interns, fellows, volunteers and contractors granted access or utilizing a VPN to access the City network. It covers the use, management, and security controls of VPNs used to access company systems, data, and applications remotely.

Abbreviations and Definitions

Virtual Private Network (VPN) is a secure private network connection built on top of a public network, such as the internet.
IT-Information Technology
MFA- multi-factor authentication

Policy

Employees who have been granted access may utilize the benefits of a VPN, which is a service managed by the City. Which means that the IT Department is responsible for coordinating installation and installing the required software on City owned or approved equipment.

1. **VPN Access Requirements**
   A. Authorization: VPN access is granted only to authorized personnel based on job roles and responsibilities. Remote access over VPN must be requested by filling out a VPN Request/Software Request Form. Requests for VPN access must be approved by the employee's department director and IT. After a period of 6 months, a renewal for VPN access may be requested for reevaluation.
   B. Authentication: All users using the VPN must authenticate using multi-factor authentication (MFA).
   C. Device Compliance: Devices used to connect to the VPN must meet the City's security standards, including up-to-date operating systems, antivirus protection, and encryption mechanisms.
   D. Minimum Password Standards: VPN users must follow the City's password guidelines, ensuring that passwords are complex, unique, and changed regularly.

2. **VPN Usage Guidelines**
   A. The employee must understand that the device being used to access the City's network and resources, once connected over VPN, is part of the City's computer network and is considered the same as any device at a person's assigned work location subject to the same regulations of use and monitoring.
   B. Acceptable Use: The VPN must only be used for business-related activities. Users should not access personal accounts, engage in non-work-related browsing, or conduct any illegal activities through the VPN. Please review and follow the Information and Systems Security Policy for details of expected behavior when accessing the City network remotely.
   C. Prohibited Activities: Users must not share their VPN credentials or allow unauthorized individuals to use their VPN access. Any such incident must be reported immediately to the IT department. The employee bears responsibility for the consequences should the access be misused.
   D. Session Management: Remote connections to the VPN will be automatically disconnected from the

City's network after 30 minutes of inactivity (idle timeout) and a maximum connection time of 8 hours. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to circumvent these limits to keep the connection open. If there is no sign-on activity for a period of 30 consecutive days, the account may be suspended from VPN access.

E. If there is a problem with VPN access, employees should report it to IT Support by sending an email to helpdesk@providenceri.gov. Please include the following information:
    1. Your name and user ID
    2. The date and time of the problem
    3. Any error messages you received

3. **Security Controls**
    A. VPN Client Software: All users must use the City-approved VPN client software. Users are prohibited from using unapproved third-party VPN applications or services.
    B. Logging and Monitoring: The IT department will monitor and log VPN usage to detect unusual activity. Logs must be retained for a period specified by the City's data retention policy and reviewed regularly for potential security threats.
    C. Security Patches and Updates: The IT department is responsible for ensuring that all VPN-related software, including client applications and servers, are regularly updated with the latest security patches and updates.

4. **Data Protection and Privacy**
    A. Confidentiality:
        1. All data accessed and transmitted over the VPN must be considered confidential and handled according to the City's data protection and privacy procedures.
        2. Secure remote access and VPN use must be strictly controlled. Control will be enforced via password authentication, token device/authenticator, and/or public/private keys with strong passphrases.
        3. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to CoP internal networks. At no time should any CoP employee, contractor, vendor, or agent provide their login or email password to anyone, not even family members.
    B. Data Loss Prevention: Sensitive data accessed via the VPN must be encrypted both in transit and at rest. Users must follow appropriate data classification and handling guidelines when using the VPN.
    C. Personal Devices: City of Providence employees must use a City owned and managed laptop or desktop to access the network by VPN. Employee personal devices are not allowed. If contractors use personal devices to access the VPN, they must ensure that their devices are protected by encryption, up-to-date software, and a security password. The City reserves the right to monitor and restrict access from such devices if they do not meet the company's security standards.

5. **Incident Response and Reporting**
    A. Reporting Security Incidents: Any suspected or actual security incidents, such as unauthorized access, VPN connection issues, or data breaches, must be reported immediately to the IT department or designated security personnel.
    B. Investigation: The IT department will investigate all reported incidents and take appropriate actions, which may include revoking access, resetting credentials, conducting a security audit, or informing legal authorities if necessary.

6. **Requirements**

A. Internet Service Provider (ISP): The user is responsible for choosing their internet service provider, setting up their internet, installing any needed software, and paying for the service.
B. Security for Remote Access: Employees, contractors, vendors, and agents who connect to the City network remotely must make sure that their connection is just as secure as if they were working in the office. They must follow the same security and privacy rules when working from home or another location.
C. Avoiding Multiple Connections: Persons with remote access to City's network should make sure their computer is not connected to any other network while using the VPN/ City network, unless it's a personal network that they fully control. For example, they should not connect to a public Wi-Fi network like the one at Starbucks.
D. Security Software: Any computer connecting to the City network via VPN must have security software installed to protect against viruses and other harmful software.
E. Split-Tunneling Not Allowed: Remote users are not allowed to set up their equipment to connect to two networks at the same time (a setup known as split-tunneling or dual-homing).
F. Vendor Equipment: Contractors or vendors working with the City must ensure their devices meet the City's security and network requirements, and they must get approval from IT. If a vendor uses a VPN to connect their own equipment to the City's network, their equipment must follow the same rules as the City's own devices. They are expected to meet the City's IT security policies and must understand that their devices are an extension of the City's network.
G. Non-Standard Equipment: Any organizations or individuals who want to use non-standard hardware or security setups for remote access to City's network must first get approval from IT.

7. **Implementation**
   A. The VPN only works with IP (Internet Protocol) and does not support other types of connections.
   B. Employees with VPN access are responsible for making sure no one else uses their connection to access the City network.
   C. VPN access is controlled with a City-issued user ID and Multi-Factor Authentication (MFA) for added security.
   D. All network traffic going to the City network is logged and tracked by user ID.

8. **Compliance**
   A. This policy regulates the use of all VPN services to the City network and users must comply with the IT Security Policies.
   B. To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service may also be disabled until the issue has been identified or resolved. In addition, service may also be disabled if there has been no activity by the user for a period of 30 days.
   C. Any City employee found to have intentionally violated the VPN Acceptable Use Policy will be subject to loss of VPN privileges.
   D. By choosing to use the CoP VPN, you hereby agree to all terms and conditions listed above.
      1. Compliance: All users of the VPN must comply with this policy. Failure to do so may result in disciplinary actions, including revocation of VPN access, progressive discipline, or legal action, depending on the severity of the violation.
      2. Periodic Audits: The IT department will periodically audit VPN access logs, configurations, and security measures to ensure compliance with this policy and recommend improvements as needed.

Related Policies:

CITY OF PROVIDENCE

Information and Systems Security Policy
Laptop Computer and Mobile Device Policy
Email Use Policy
Electronic Signatures
Artificial Intelligence (AI) Policy

Other Related Information:
VPN Request Form
City of Providence Technology Password Guidelines