****

**VIRTUAL PRIVATE NETWORK POLICY**

**Version History:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. No.** | **Release Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 3rd Sep 2013 | First Draft | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.0 | 30th Sep 2013 | Initial Release | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.1 | 29th July, 2015 | Update VPN policy for Employee Access | Ajeet Singh | Saket Madan | Ajay Kr. Zalpuri |
| 1.2 | 3rd Dec 2018 | Update section 3 for VPN policy for complex password | Ajeet Singh | Saket Madan | Ajay Kr. Zalpuri |
| 2.0 | 4th March 2019 | Update section 4 for policy compliance | Rahul Raj | Saket Madan | Ajay Kr. Zalpuri |
|  |  |  |  |  |  |

**Table of Contents**

[1. Objectives 4](#_Toc79414371)

[2. Scope 4](#_Toc79414372)

[3. Policy 4](#_Toc79414373)

[4. Policy Guidelines 4](#_Toc79414374)

[5. Policy Compliance 6](#_Toc79414375)

# Objectives

The purpose of this policy is to provide guidelines for Remote Access connections to organization’s corporate network.

# Scope

This policy applies to all SVAM employees. This policy applies to implementations of VPN

# Policy

* Approved SVAM employees and authorized personnel may utilize the benefits of VPNs.
* It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to organization’s internal networks.
* VPN use is to be controlled using corporate credentials tied in with Active Directory.
* VPN gateways will be set up and managed by the network administrator.
* All computers connected to organization’s internal networks via VPN, or any other technology must use the most up-to-date anti-virus software that is the corporate standard (this includes personal computers).
* VPN users will be automatically disconnected from SVAM network after thirty minutes of inactivity. The user must then login again to reconnect to the network.
* VPN account will be removed as soon as the Employee leaves the Company.
* Complex password policy implemented with following combination
  + *VPN Password contains following four categories:*
    - *English uppercase characters (A through Z)*
    - *English lowercase characters (a through z)*
    - *Base 10 digits (0 through 9)*
    - *One special character (for example, !, $, #, %)*
* It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to SVAM internal networks.
* VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

# Policy Guidelines

**Advantage of Telecommuting or Teleworking**

* Employees are generally less stressed, happier, and more productive working at home, while employers' benefit from less employee absenteeism, increased output and retention of good employees.
* Employees save time and money by not commuting, and employers save office space.
* Employees can live anywhere, and employers have a vastly larger pool of potential workers to choose from.
* Employees and employers both benefit from greater flexibility in work schedules.
* Working at home can offer a short-term solution for injured employees or those returning to work after a disability, which benefits both employees and employers.

**Disadvantage of Telecommuting or Teleworking**

* Employees may not feel like part of the team, and supervisors in the office may have difficulty building a solid working relationship with remote workers
* Employees may not have access to resources and learning opportunities to help them grow and develop in their profession, and employers will miss out on the potential these employees could offer in the future.
* Collaborative projects and brainstorming can be more difficult.
* If the employee is several time zones away, meetings and conference calls can be difficult to arrange.
* Employees may feel like they can’t escape work, while employers may feel that it’s more difficult to know when employees are working.
* Less motivated and less skilled employees may flounder when working on their own without a built-in support system, while supervisors may have a difficult time coaching and trusting employees who encounter difficulties while on their own.

**Risk of Telecommuting or Teleworking**

* Installing company equipment in remote offices gives an edge for keeping the system, software, and security protection up-to-date, and a secure virtual private network (VPN) is essential to encrypting and protecting our company system.
* Offer help through IT help desk or other experts; allow in-house experts to remotely log in and assist employee with any computer or security issues to control the fixes.
* Allow remote employees limited access to sensitive data through credentialing, providing access only to data needed for the job.

# Policy Compliance

SVAM IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions- Any exception to the policy must be approved by the line Manager/ IT Manager in advance.

Non-Compliance- An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.