CresTech®
YOUR TESTING PARTNER
A CMMI Level 3 SVC Company

VPN & Remote Access Policy

<table>
<tr><td colspan="3">Policy Category:</td><td colspan="2">IT</td></tr>
<tr><td colspan="3">Policy Name:</td><td colspan="2">VPN & Remote Access Policy</td></tr>
<tr><td colspan="3">Version:</td><td colspan="2">1.0</td></tr>
<tr><td colspan="3">Effective Date:</td><td colspan="2">1-August-2015</td></tr>
<tr><th colspan="5">Version History</th></tr>
<tr><th>#</th><th>Description of Change</th><th>Date of Release</th><th>Version No.</th><th>Approved by</th></tr>
<tr><td>1</td><td>Release</td><td>1-August-2015</td><td>1.0</td><td>Lalit Jain</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

CresTech Software Systems Pvt. Ltd
www.crestechglobal.com

Objective:

The objectives of this policy with regard to the protection of information system resources against unauthorized access from remote locations are to:

- Minimize the threat of accidental, unauthorized or inappropriate access to CresTechs' Network,
- Minimize The CresTech network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources,
- Minimize reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality.

Policy Statement:

The CresTech resources are assets important to the CresTech business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. It is the CresTech policy that appropriate remote access control measures are implemented to protect its information system resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

Scope:

The scope of this policy applies to:

- The CresTech personnel, temporary staffs, contractors and authorized remote users
- The CresTech resources from a remote location, Information system resources, including data networks, LAN servers and personal computers
- personal computers and/ or servers authorized to access The CresTech data networks.
- Third parties shall also adhere to this policy.
- Remote access connections used to do work on behalf of The CresTech, including reading, sending email and viewing intranet web resources from all types of equipment.

General Rules & Principles of Virtual Private Networks (VPNs)

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to The CresTech 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.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- All computers connected to The CresTech Software Systems Pvt. Ltd. internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard

- Remote access users will be automatically disconnected from The CresTech network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- By using VPN technology with personal equipment, users must understand that their machines are a extension of The CresTechs' network, and as such are subject to the same rules and regulations that apply to The Smart Software Testing Solutions owned equipment, i.e., their machines must be configured to comply with The Smart Software Testing Solutions' information security policies.
- Remote access provided to third parties in order to e.g. remotely administer systems should be restricted to particular IP addresses, should involve a named account and the account should be disabled when it is not in use.
- All security incidents, including actual or potential unauthorized access to the CresTech systems via remote access, should be reported immediately to the IT Manager.

Disciplinary Process

- The CresTech Software Systems Pvt. Ltd. reserves the right to audit compliance with this policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with The CresTech Rules and Disciplinary Code as amended from time to time. Disciplinary action may ultimately lead to dismissal.

Deviations from Policy

- Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy will be reported to the IT Manager.