Remote Access Policy

Johnson & Associates

October 9, 2015

IT Department Members

- Christopher Brewer
- Mauchel Barthelemy
- Nicholas Gikonyo
- Victoria A. Johnson

Johnson & Associates

REMOTE ACCESS POLICY MANUAL

Section 1: Introduction

Johnson & Associates (also referred to as "the company") engages in a mission to provide quality criminal defense services for the Philadelphia community. In order to maintain such a critical task, we commit to use cutting-edge and secure technology. It is in the same line of effort we produce this Remote Access Policy to enhance our vision.

Johnson & Associates employees and contractors are all subject to comply with contents or provisions within this document. We establish this policy and related policies in an effort to ensure the transparency and provide information on using computer systems remotely. The goal is to protect the technology, data and information assets of Johnson & Associates.

This Remote Access Policy explains authorized users' roles and responsibilities, policy directives, compliance and references to related security policies. Furthermore, it provides company employees and contractors a chance to thoroughly understand Johnson & Associates rules regarding remote network access, physical/hardware usage/security, and authentication requirements. The policy also points out the consequences if employees and contractors fail to comply with designed rules.

Section 2: Scope

This policy applies to all employees and contractors of Johnson & Associates who are authorized by management and IT to use remote access technologies (also collectively referred to "authorized users"). It applies to company issued laptops, company issued mobile devices, personal mobile devices and personal computers that have been evaluated and approved by the company for remote connectivity (collectively referred to as "authorized devices").

The policy applies to all remote access connections used to perform duties for or on behalf of Johnson & Associates including sending and receiving emails, accessing the intranet, accessing files and systems on the company's network using technologies that include, but not limited to, VPN, Remote Gateway Server and Citrix.

Section 3: Roles and Responsibilities

At Johnson & Associates, our rules and responsibilities are governed by the Principle of Least Privilege to all users including management, attorneys, accountants, system engineers, and other employees. This rule ensures that users are granted only enough access needed to perform their job.

- Management at Johnson & Associates will review and provide approval for users and contractors requesting remote access to our systems via secured Virtual Private Networks (VPNs).
- Only lawyers and systems engineers should have remote access to the terminal and file servers. It is the managers' responsibilities to ensure that other employees, other than engineers and help desk personnel, have only access their local machines and applications servers pertaining to their jobs.
- Only systems engineers should have administrator rights across all server platforms.
- All remote access users will be automatically prompted to change their passwords every two months and it is their responsibility to change their passwords accordingly. Please review the *Password Policy* for details
- All remote access permissions will be reviewed by the manager when an employee transfers within Johnson & Associates or job duties change. Contractor permissions will be reviewed by their supervising manager every two months.
- Department managers and supervisors are responsible for notifying the company, in a timely manner, any employee and contractor termination according to the *Employee and Contractor Termination Policy.*
- Authorized users are responsible for preventing unauthorized users from accessing their authorized device when connected to the company's network and securing their login information.
- Authorized users are responsibility for reporting knowledge of anyone using remote access without approval, sharing passwords or using it for non-business purposes.
- IT department manager will monitor and log all remote session information including, but not limited to, IP address, device information, connection time, connection period and resources accessed.

Section 4: Policy

Remote Access is provided for approved business use only. Any other use, including leisure use and illegal activities, is prohibited. Authorized users are fully responsible for actions performed by unauthorized users on their device and/or account. For additional information on various remote connection technologies, how to connect to the company's network remotely and how to obtain approval, please visit www.johnsonassociates.com/remote.

Requirements:

- Authorized Users must use their approved login and password and shall protect that information from all unauthorized use.
- Personal computers and mobile devices used to connect to the Company's network must be approved by the IT department and meet the standards set in the *Personal Devices Policy*.
- Authorized devices must have the latest antivirus definitions, encryption and software updates. For details, see the *Acceptable Encryption Policy*.
- Authorized devices must use Company approved technologies for remote connectivity and run only approved software.
- While connected to the company's network, users must only access systems and data approved for access remotely.
- Remote sessions must be initiated from trusted and secure connections only. Access from public or open wireless connections is strictly prohibited.
- Authorized devices lost, stolen or compromised should be reported to the company as soon as possible.
- Company data accessed while working remotely shall not be stored or copied on to the remote device.
- Authorized users are only allowed one remote session on one authorized device at a time.

Section 5: Compliance

Johnson & Associates will conduct periodic audit and run reports on accounts and devices used for connecting to the company from remote locations to verify compliance with this policy. This may include verify security settings, software updates, checking for company data and access levels. Violation of this policy may result in disciplinary action, including revoking remote access rights and termination.

Section 6: References

Please review the following policies for additional information:

Acceptable Use Policy
Acceptable Encryption Policy
Personal Device policy
Password Policy
Employee and Contractor Termination Policy