Sources Concerning: Remote Access As of 4/3/20.

DISCLAIMER: *While we attempt to assert that this document includes all information available on the ffiec.gov website as of the date listed above, we offer this as an aid to audit and consulting Clients, and in no way warrant this as being all-inclusive, complete, or thorough. Please use at your own risk.*

Business Continuity Planning Booklet:

Other Policies, Standards and Processes:
Remote Access
https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/other-policies,-standards-and-processes/remote-access.aspx?prev=1 (Accessed 4/3/20)

Remote access policies and standards should be established as an important part of BCP implementation. In the event of a disaster, personnel may be able to work from a remote location and vendors may be allowed remote access to back-up facilities. As such, remote access guidelines should be developed addressing acceptable configuration and software requirements for certain remote devices that may introduce security risks. Remote access policies should address various security guidelines including prior management approval requirements, controls for third-party access, and virus controls. If employees are allowed to use personal computers for remote access during a disaster, management should ensure that only secure connections are used e.g., VPN. In addition, clear guidance should be established and disseminated to employees regarding appropriate procedures to follow when accessing or transmitting confidential information from a remote location.

Information Security Booklet:

Section II: Information Security Program Management:
II.C.15(c) Remote Access
https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic15-logical-security/iic15(c)-remote-access.aspx?prev=1
(Accessed 4/3/20)

Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely. Management should employ the following measures:

- Disable remote communications if no business need exists.
- Tightly control remote access through management approvals and subsequent audits.
- Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use.
- Log and monitor all remote access communications.
- Secure remote access devices.
- Restrict remote access during specific times.
- Limit the applications available for remote access.

- Use robust authentication methods for access and encryption to secure communications.

There are several methods to provide remote access to employees. A prevalent form of remote access is through a VPN, which provides employees with a remote connection to the institution's network through a secure channel.
The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. VPN provides an encrypted isolated "tunnel" or connection between a remote user's computer and the internal network.

Because VPN connections provide access to sensitive internal networks, the connections require additional authentication from the remote user. Use of physical token devices is a common method that can provide one-time passwords to strongly authenticate remote users.

While VPNs effectively connect the remote computer to the internal network, other alternatives provide virtual desktop capability. In these cases, the remote computer connects to a special purpose software system (sometimes a website), authenticates the user, and establishes a secure connection to an internal network server. That server establishes a local internal network desktop session and connects it to the screen, keyboard, mouse, and speakers of the remote computer. This is an actual remote control environment, where the remote user's actions have the same effect as if connected to an actual internal network desktop. The remote control configuration may permit file transfer between the remote and internal computers. If the remote access method allows users to store sensitive institution information, management should consider limiting this access to institution-owned devices.

Other methods of remote access are available, including remote control software and third-party services, file transfer software (e.g., FTP), conferencing/session sharing tools, and other remote desktop software. Management should conduct a risk assessment and implement appropriate controls before adopting any remote access solution.

If the institution allows employees to use authorized remote access methods with institution-owned devices, management should implement the following mitigating controls:

- Prevent users from installing software on the devices.
- Prohibit users from having administrative privileges on the devices.
- Use firewalls, host-based IDS, and packet content filtering to identify, monitor, and limit remote access activities.