	Georgia Technology Authority	
Title:	**Technology Guideline for the Remote Worker**	
PSG Number:	**GS-21-001**	
Issue Date:	**7/1/2020**	**Effective Date: TBD**
Synopsis:	To ensure that teleworking is performed safely from an information security perspective	

PURPOSE

To provide state agencies and employees with detailed processes and procedures that will assist in working from a remote (virtual) environment; to enable state business to be conducted remotely while ensuring the protection of state equipment, assets, data, and information. These measures include, but are not limited to: clearly addressing security requirements; implementing end-user training and awareness education; describing processes for and the means by which employees will purchase or borrow the equipment and software they use; and establishing a maintenance schedule and support network for employees working away from state facilities.

SCOPE and AUTHORITY

GTA's statutory authority to establish policies and standards per O.C.G.A. 50-25-4 (a) (10) and Information Technology Policies, Standards and Guidelines PM-04-001.

GUIDELINE

A. Security and Confidentiality

State agencies should implement telecommuting security controls in proportion with risk and exposure. These security controls are to protect against theft of enterprise equipment, unauthorized disclosure of information, misuse of equipment, or unauthorized access to information assets. Controls could include:

1.) ***Baseline Recommendations:*** The following are baseline requirements for all employees working from a virtual environment.

- the use of public computers (e.g., library) to access any state-owned IT resources is prohibited.
- Virtual employees must use a secured Wi-Fi network to connect to or access any state-owned resources.
- Computing devices must be secured with a password-protected screensaver enabled, as applicable. Users must lock the screen or log off/sign out of the device when the device is unattended.
- Personally Identifiable Information (PII) should be stored on network drives and/or in application databases with proper access controls (i.e., user ID/password) and made available only to those individuals with a valid need to know.
- Sensitive and/or moderate data must be encrypted.
- Computer and/or devices that store state data should not be left in a car.
- State data should not be stored on a personal device unless approved by the agency.
- Agencies should create a reference of whitelist and blacklist apps.
- Agencies must enforce strong password policies and requirements.

- Employees should be given only the level of privilege necessary for them to do their jobsMulti-Factor Authentication (MFA) is highly recommended for all users and required for network access to privileged accounts and sensitive data.
- Administrative access should be limited.
- All workstations that connect to state systems should have up-to-date firewall and antivirus software installed.
- IT security training should be required by agencies to keep remote users aware of requirements and responsibilities.

2.) ***Personal Devices (BYOD/PC)***

As a best practice, it is recommended that state agencies prohibit the use of home computers and personal technology devices (Bring Your Own Device (BYOD)) by state employees to access state systems. From a support and cybersecurity standpoint, using home computers and personal devices is strongly discouraged. Although enterprise standard SS-12-002 Non-State Technology and Computer Devices delegates the decision to use personal computing devices to individual agency leadership, it is important that agencies understand that they assume all risk involved in this practice. Agencies should verify that all security controls are configured and updated. It is highly recommended that any agency choosing to approve the BYOD/PC practice adhere to the following guidance.

- Restrict use of personal devices for:
    - Employees whose job involves the transfer of state funds.
    - Employees whose job involves accessing sensitive data.
    - Employees who have administrative/privileged accounts.

3.) ***Removable Storage Devices, Media and Printed Material***

There is risk of disclosure of sensitive information through careless storage, disposal or reuse of media, devices. Formal processes should be established to minimize this risk. State employees should consult their agency Information Security Officer (ISO) for a list of allowable storage devices/services, required protective measures, and disposal procedures.

Best Practices:

- Storage media containing sensitive information must be stored in a locked and secured place.
- No portable storage device should store any sensitive information without suitable physical and technical protective measures in place.
- State-owned sensitive data must not be stored or transmitted from a personal storage device.
    - Any exception should be approved by agency leadership and the personal storage devices should be provisioned by the agency's IT staff.
- Equipment, information, or software should not be taken out of the office environment without prior authorization.
- The contents of removable media within the home office should be permanently destroyed or rendered unrecoverable when no longer required in accordance with applicable state, federal, or agency record retention requirements.
- Storage devices such as hard disk drives and other media (tapes, diskettes, CDs, DVDs, personal electronic devices, or other devices that store information) containing state information should be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information.
- Employees must use only state-authorized cloud-storage services to store state

information.

4.) ***Protecting Printed and Written Materials***

This section provides guidance on disposal of printed materials containing sensitive information within a remote office environment. Information security policies do not change when an employee works from home. It is the duty of the employee to safeguard sensitive information, including PII. All agencies should ensure that remote workers understand the proper way to destroy sensitive printed materials they may have at remote locations. State employees should consult their agency ISO for proper printing and disposal procedures.

Appropriate physical security of teleworking sites is necessary to reduce or eliminate the likelihood of the loss of work-related information or equipment. Teleworkers are responsible for the security of all official data and protection of any state property when teleworking.

Best Practices:

- Agencies must identify employees who should have access to sensitive information.
- Employees and agencies must know the sensitivity of documents, and make sure they are appropriately marked to help mitigate the risk of unauthorized disclosure.
- If possible, avoid printing sensitive electronic documents and access them only within the state/agency network.
- Printed documents containing sensitive information must be stored in a lock and secured place.
- Family members should be prevented from accessing documents containing sensitive information.
- Agencies should deliver regular security awareness training.
- The contents of printed documents within the home office should be permanently destroyed or rendered unrecoverable when no longer required in accordance with applicable state, federal or agency record retention requirements.

5.) ***Teleconferencing/ Videoconferencing Security***

On April 2, 2020, GTA OIS released a guide detailing teleconferencing security best practices. The guide detailed recent "ZOOM BOMBING" redirect attacks, where malicious individuals join teleconferences uninvited and disrupt meetings with explicit video and/or audio. Since the guide was released, a number of recent developments involving Zoom security vulnerabilities have taken place:

- April 16, 2020 – Two new Zoom exploits uncovered. With one, a researcher discovered that previously recorded Zoom sessions may live on the Zoom cloud for hours, even after being deleted by the user. The researcher also discovered it could access these recorded meetings via unsecured links. In response, Zoom introduced updates to prevent malicious actors from exploiting the vulnerabilities and changed its "Record to Cloud" default setting to request that the uploading user add a password to the video file.
- April 15, 2020 – A Windows-specific zero-day vulnerability for sale for $500,000 was discovered on the dark web. The vulnerability is a Remote Code Execution (RCE) exploit but requires the hacker to be in a call with the target.
- April 13, 2020 - 500,000 Zoom accounts were sold on hacker forums. Over 500,000 Zoom accounts are for sale on the dark web and hacker forums, often for less than a penny each. In some cases, the accounts are being given away for free.

Given that Zoom's security issues continue to evolve, it is important to consider when using Zoom is appropriate. On April 10, 2020, the U.S. Department of Defense (DOD) restricted the use of Zoom to Zoom for Government accounts only. Zoom for Government is a paid service tier of the software. The DOD notes that their users may not host meetings using Zoom's free or commercial offerings and may only use Zoom for Government to discuss “publicly releasable DOD information not categorized as ‘For Official Use Only.’” Zoom users can verify the version by visiting the Zoom support page: https://support.zoom.us/hc/en-us/articles/201362393-Viewing-the-Zoom-version-number. It may also be advisable to contact the meeting host to inquire about security measures taken.

It should be noted that even in the Zoom for Government platform, the company cannot offer assurances for how it protects chats, audio, and video from meetings. Zoom’s advertised “end-to-end” (E2E) encryption architecture does not actually meet the standard definition of E2E. Zoom uses TLS, also known as transport encryption, which is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings. Therefore, meetings would stay private from anyone spying on the user’s Wi-Fi, but not from Zoom itself. In addition to encryption concerns, the company also admitted to inadvertently routing some calls through China. In a public statement, Zoom CEO Eric S. Yuan said, “In February, Zoom rapidly added capacity to our Chinese region to handle a massive increase in demand. In our haste, we mistakenly added our two Chinese datacenters to a lengthy whitelist of backup bridges, potentially enabling non-Chinese clients to connect to them.”

- Agencies should consider their use cases for Zoom and either lock Zoom down using best practices or consider using alternate platforms such as Microsoft Teams, Skype, Cisco WebEX, or BlueJeans.

B. Remote Access

1.) VPN Gateway:

Virtual Private Network (VPN) gateways create secure access from the employee device to the VPN gateway and onward to the internal network. In this way, the enterprise-level cybersecurity measures are extended to the VPN, which acts as a secure tunnel for employees to work through. Some VPN gateways can even extend the firewall rules to the employee’s computer no matter the location through the use of a portable device—an advantage when working virtually on business. VPN gateways offer several useful telework features, but while communication is protected through a VPN gateway, the employee’s computer could still be at risk of transmitting infected data if the computer itself is compromised. VPN gateways should be used only in conjunction with properly configured, state-owned hardware to maintain high security standards and minimize the risk to the internal network.

2.) *Portals:*

In this method, telework employees access data and applications through a browser-based webpage or virtual desktop. All applications and data are stored on the portal’s server and cannot be downloaded or saved on an employee’s device without permission. This is a good way to keep control over who is accessing data and how it is used. The danger with portals depends on what permissions the employee has while accessing the portal. If the portal allows an employee to access other areas of the internet while connected, it could provide an unintended avenue for bad actors to access the network. It is safer to restrict employees’ access to other programs while the portal is in use. The more access an employee has, the less secure the connection becomes.

3.) *Remote Computer Access Service:*

Remote computer access services allow an employee to remotely control a computer physically located at a state facility via an intermediate server or third-party software. When the two computers are connected, applications and data remain on the office computer, and the network’s cybersecurity measures are enforced. The remote device acts as a display for the work performed on the office machine. Due to the direct access, remote desktop connection is considered high risk in cybersecurity terms. Proper configuration is critical. When set up correctly, communication between the two computers is encrypted for the data's protection, but it is also encrypted from the firewall(s) and threat detection. Regardless of how good the cybersecurity measures are, if the employee's home computer does not have the same protections as the office workstations, malicious data can slip into the network unnoticed during a remote desktop connection. Agencies should not allow remote data transfer unless both endpoints are state-owned (managed) devices.

4.) *Direct Application Access:*

Direct application access is probably the lowest risk to cybersecurity measures out of all the remote access methods because it is best used only with low-risk applications. In this method, employees can remote into a single application, usually located on the perimeter of the network, such as webmail. The employee does not have access to the entire network, allowing them to work on select applications without exposing the internal network to danger. Though there is much less risk posed by direct application access, it generally does not allow for extensive work to be done. There is very little connection to data on the network and little ability to take data to another application if needed. It is best used when traveling or on a mobile device where complete access to the network is not necessary.

5.) *Virtual Desktop Infrastructure (VDI) (Cloud-Based Compute Resources)*:

Just as virtualization enables IT administrators to host numerous software-based servers on one hardware unit, virtual desktop technology delivers rich work environments to endpoints, with the actual applications and data residing on a central server that never leaves the data center. With VDI, sensitive information never touches the endpoint, and users may manipulate data and work on applications only after strong authentication. Standard desktop images are easily managed, monitored, patched, and upgraded by IT, with no need to worry about the endpoint device. In many cases, users can access their virtual desktops via any web browser, which enables seamless telecommuting for home workers and easy integration of contractors and consultants. The virtual desktop environment can be adjusted to fit the smaller screens of smartphones and other mobile devices as well to enable anytime/anywhere productivity.

C. <u>Acceptable Use</u>

The goal of the Acceptable Use section is to establish appropriate and acceptable practices and responsibilities regarding the use of IT resources, which will protect proprietary, personal, privileged, or otherwise sensitive data.

- Every user must avoid all activity that compromises the security, performance or integrity of IT resources, or that negatively impacts the IT resources or other users.
- Users must only use IT resources within the scope of their employment or contractual relationship with the state and must agree to abide by the terms of state policies.
- Users shall promptly report to their supervisor and/or the service desk all security incidents, disruption of service, actual or suspected theft, loss, and/or unauthorized disclosure of IT resources.
- Users may access, use or share IT resources only to the extent necessary to fulfill assigned job duties.
- All IT resources must be handled with due care and confidentiality. Users who create, receive, process, edit, store, distribute, or destroy IT resources which are confidential, sensitive in nature, and/or governed by federal or state laws, rules or regulations must understand their responsibilities to protect such information.

- All computing devices, which include personally owned devices, that connect to the state of Georgia internal network must first be authorized.
- Use of another user's password or any other authentication capabilities is strictly prohibited.
- User privileges must not be elevated without formal approval by authorized personnel.

Prohibited Activities:

- Violations of any copyright, trade secret, patent or other intellectual property, or any similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" or any other software products that are not licensed for use by the state.
- Careless introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, and e-mail bombs).
- Revealing an account password to others or allowing others to use one's account (including family and other household members).
- Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation, or which may compromise the security of the state IT resources.
- Sharing or storing IT resources via unauthorized cloud services.

E. <u>Technology Management Support and Services</u>

As IT resources become strained due to the shift to a remote work environment to combat the COVID-19 pandemic, quickly remediating critical network vulnerabilities becomes more difficult and more important. If security teams work too hastily and without a plan, their corporate systems and employee devices could face additional risk due to incomplete patching or careless use of remote administration tools.

1.) ***Patch Management***

Patching of systems must be attended to, even as IT teams must also manage assisting an influx of newly remote employees, upgrading infrastructure to handle the increased remote workforce, and monitoring their environments for signs of a security event. In some cases, patching may be intentionally delayed due to fear of downtime. Following are best practices to consider when patching systems remotely:

- Discuss potential user impact of patch with stakeholders prior to rollout. Be sure to test patches in advance and confirm that users will not be affected.
- Send notifications to users across multiple internal channels (e.g., email, calendar invite, internal message board) to advise of patches and any expected changes to their systems.

- Consider investing in a cloud-based, automated remote patch management solution. Patch management solutions can securely push patches from a central server across scattered networks of varied devices. As long as an agent machine has internet access, it will be able to send results and receive updates using the cloud. Keys for manually installing agents onto machines that are disconnected from the network can also be created and distributed.

- Perform rolling updates with a small percentage of devices updated first and others following later. This approach allows for time for issues to be identified and fixed before the entire fleet of devices is updated.

- If a laptop that is not attached to the corporate VPN needs to be patched, consider placing the machine in quarantine and forcing it to go to a remediation server to receive patches. The process is followed by forcing the machine into a separate network segment to receive patches before it is allowed through the firewalls.

2.) ***Remote Management Tools***

Remote administration tools used by IT staffers to troubleshoot devices could leave an open door for attackers if they are able to obtain an admin's credentials. At the 2020 RSA conference, the FBI revealed that Remote Desktop Protocol (RDP) constitutes 70 to 80 percent of the initial foothold that ransomware actors use when infecting an organization. The following are best practices to consider when utilizing remote management tools:

- Place RDP servers and other remote management tools behind a VPN, use host-based security measures, and implement multi-factor authentication (MFA) on admin accounts.
- Minimize number of admin accounts and ensure that admin accounts are unique to one system. Attackers can potentially re-use credentials to move laterally. Microsoft's Local Administrator Password Solution (LAPS) is a means to avoid this scenario across the organization with central management of unique local administrator credentials.
- RDP Gateway on Windows Server provides logging, TLS certificates, authentication to the end device without exposing it to the internet, and authorization to internal host and user restrictions.
- Lock out users and block or timeout IPs with too many failed logon attempts.
- Implement measures like least privilege/role-based access control policies and MAC/IP filtering.
- Verify and test that the servers can keep up with the demand of an increased number of concurrent remote workers.
- Confirm that the corporate VPN is patched with the latest updates.
- Communicate VPN usage guidelines so employees know which services can be accessed only through VPN.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Telework and Remote Access (SS -08-037)
Software Management Standard (SM-19-001)
Multi-Factor Authentication Policy (PS-19-001)
Network Security Controls (PS-08-027)
Network Security (SS-08-047)
Network Access & Session Controls (SS-08-048)
Access Control (PS-08-009
Appropriate Use of Information Technology Resources (PS-08-003.2)
Appropriate Use and Monitoring (SS-08-001)

TERMS AND DEFINITIONS

TBA