Remote Working and Mobile Computing Device Information Security & Privacy Policies

[This document is provided free to a single organization to use for its own organization's internal policies. If you would like to recommend to someone else that they could find value in downloading this resource, please point him/her to https://privacysecuritybrainiacs.com/free-resources/remote-working/ so he or she can then download directly from our site. This allows us to not only better manage our intellectual property, but it also helps us to understand, from the number of downloads, the topics that are of most interest to the population in general.

Do you have suggestions for edits to this document? Or suggestions for other policy statements to add to this document? Or any other type of feedback about this document? Please send to: Feedback@privacysecuritybrainiacs.com.

Instructions:

1. **This document contains a compilation of many possible remote working and mobile computing device policy statements. Some organizations may not need all these policy statements. It is important for you to use and appropriately modify the statements in this document to best fit your organization's type of business, industry, environment, location(s) and legal requirements, and to delete the other policy statements that do not apply to your organization.**
2. **Carefully review and edit as necessary to best fit your organization's business activities.**
3. **You may have some of these policy statements in some of your other existing policies. If so, it will usually best to remove the associated policy statement verbiage and replace it with a statement pointing to the existing policy where the associated policy statement is located. Some of the policy statements found in this document do just that; you can use them as models.**
4. **Edit department names, position titles, names of referenced policies, procedures, standards, and any other information as needed for your organization's business practices.**
5. **Replace company information by changing "Company X" to your company name throughout the document.**

6 Delete statements that do not apply to your organization, based upon your work environment, services, products and legal compliance requirements.

7 Edit throughout as appropriate to your organization, changing terminology as necessary and deleting sections that do not apply to your organization.

8 Make sure to specifically consider all bold and highlighted passages, and change, as necessary, to what is most appropriate to your organization. Then remove the highlighting from the passage.

9 All the policies, and necessary referenced separate supporting procedures and forms, should accurately reflect the specific titles, needs, and actual activities, of your organization, and should be edited accordingly throughout the text.

10 If you make the decision that a policy statement does not apply to your organization, simply delete the associated text, and/or if appropriate, note that the topic is not applicable to the services and/or products that your organization provides.

11 Delete this section in brackets, as well as any bracketed sections below, after performing edits and finalizing.]

Table of Contents

Company X employees, contractors and third parties must ensure they appropriately establish information security and privacy protections within every area where they work when they are outside of the work facilities. To support such protections, the following policies must be followed.

1. Mobile Computing Work Areas

1.1 All **Company X** employees, contractors and third parties must remove personal information and other confidential information, in any form, from the tops of their desks and other accessible locations whenever any type of work area, in any location, is unattended and unlocked. This includes removing and securely storing away all confidential papers, removable storage media, mobile computers, and other types of media with access to **Company X** systems and information.

1.2 Lock computing devices, storage devices, confidential papers, and other business artifacts, within in-room hotel safes or take with you when leaving hotel rooms, remote meeting rooms, and other areas where unauthorized access and/or use could occur.

1.3 All confidential and personal information on whiteboards, flipcharts and all other types of viewable work boards in work areas outside of **Company X** controlled facilities must be removed or cleaned free of information after use if others who are not authorized to see the information will possibly be able to view it.

1.4 All workstations and computing device screens must be clear of personal information or other confidential information when unattended to prevent inadvertent or deliberate viewing by unauthorized individuals.

1.5 All **Company X** employees, contractors and third parties must use **Company X** approved privacy screen shields to help prevent unauthorized viewing on laptops, tablets, smartphones and other mobile and remote computing device screens.

1.6 Screensavers on all remotely-used and mobile workstations and computing devices must be configured to hide the contents displayed on workstation and computing device screens and lock the workstation after an idle period of no more than ***5 minutes, or the value that is acceptable for your organization***. The screensaver must require a strong password to unlock the screen.

1.7 **Company X** employees, contractors and third parties must lock their workstation and computing device screens when leaving their work areas in home offices and other remote work areas.

1.8 **Company X** employees, contractors and third parties must ensure that unattended computing and storage equipment outside of **Company X** controlled facilities have appropriate data, applications, systems and physical protection to prevent unauthorized access.

1.9 **Company X** employees, contractors and third parties must ensure that all "smart" Internet of Things (IoT) devices (such as Alexa or Google Home types of personal assistant devices, smart TVs, smart toys, home video monitoring devices, etc.) in the vicinity of where work is being performed are

turned off and completely shut down (e.g., unplugged, etc.) in accordance with the **Company X** ***Remote and Mobile Computing IoT Device Use Procedure*** to prevent work activities from being recorded or captured.

1.10 Access to remote areas containing personal information, other types of confidential information, and computing hardware used at least some of the time for business purposes must be restricted in accordance with the ***Secured Area Access Procedure.***

1.11 All hardcopy and digital business-related information in remote work areas must be securely disposed of in accordance with the **Company X** ***Electronic Data Storage Device Disposal Procedure***, ***Computing Device Disposal Procedure***, and ***Hard Copy Information Disposal Procedure***.

1.12 All remote work areas are subject to work area audits in accordance with the ***Work Area Security and Privacy Review Procedure***.

2. Mobile Working Management & Responsibilities

2.1 Only appropriately authorized employees, contractors and third parties are allowed to do mobile and remote working activities, in accordance with the ***Mobile Working Approval Procedure***.

2.2 **Company X** employees, contractors and third parties authorized for remote access must provide documentation up request validating that they have participated in training prior to obtaining remote access. Training must cover, at a minimum, the following in accordance with the **Company X** ***Awareness and Training Policies***. ***[NOTE: Your organization should follow your training and awareness policies for these activities; those policies are not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]***:

1. Securely accessing, storing and transmitting personal information and other confidential information through mobile devices and from remote locations.
2. Remote device/media protection practices that reinforce remote and mobile computing policies and procedures.
3. Activities that are prohibited, including the transmission of personal information or other confidential information over open public networks (including email), downloading personal information to public or remote computers, and other types of high-risk activities.
4. Acceptable use of personally owned computing and digital storage devices.
5. Phishing and other types of social engineering tactics.

2.3 All employees, contractors and third parties authorized to work remotely and using mobile devices for work activities must receive regular security and privacy training in accordance with the **Company X** ***Awareness and Training Policies***. ***[NOTE: Your organization should follow your training and awareness policies for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]***

2.4 All work performed away from **Company X** facilities for **Company X** business purposes must be performed in a secure manner, taking all precautions to safeguard information and access to **Company X** systems.

2.5 While outside of **Company X** facilities, **Company X** employees, contractors and third parties who access **Company X** systems, networks and other information assets, are responsible and accountable for the physical protection of the computer resources they use and for safeguarding the digital information they access, store and transmit remotely.

2.6 Remote workers must connect to the **Company X** network using the company-issued Virtual Private Network (VPN) to access any work accounts.

2.7 Remote workers using their home wireless (WiFi) network routers should ensure their router is updated with the most current software and secured using a strong password or passphrase that complies with the **Company X** ***Authentication Policies***. ***[NOTE: Your organization should follow your training and awareness policies for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]***

2.8 Employees, contractors and third parties must not connect to public WiFi networks to access work accounts unless using the **Company X** approved and provided VPN.

2.9 Employees, contractors and third parties must segregate their home WiFi network so that **Company X** connections are made through a separate WiFi sub-network of the home WiFi network that is used for non-business activities, and by others within the home. See the ***Wireless Access Management Procedure*** **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]** for information about how to accomplish this.

2.10 Employees, contractors and third parties must keep devices with them at all times, or stored in a secure location when not in use. Set auto log-out for ***30 minutes, or the value that is acceptable for your organization*** in case you walk away from your computer and forget to log out.

2.11 Limit access to the device you use for work. Only the approved and authorized employee, contractor or third party should use the device (family and friends should not use a work-issued device).

2.12 Remote access to **Company X** information assets will be tracked in accordance with the ***Mobile Working Tracking Procedure***.

2.13 The computing devices **Company X** employees, contractors and third parties use to perform work and business activities from remote locations are subject to audits in accordance with the ***Mobile Working Audit Procedure.***

2.14 **Company X** contractors and third parties may use remote-access solutions and technologies only if necessary to fulfill contractual requirements and with the contractually required safeguards in place. Specific safeguards must be outlined in the associated contracts they have with **Company X**.

2.15 Remote access to **Company X** hardware, applications and systems must be restricted and secured, using **Company X** approved security tools, according to the ***Wireless Access Management Procedure***. **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

2.16 Multi-factor authentication must be used for authentication into **Company X** systems, networks and applications from remote locations and mobile computing devices in accordance with the **Company X** ***Authentication***

Policies. **[NOTE: Your organization should follow your own Authentication Policies; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document. Change the title to match your own organization's authentication policy.]**

2.17 The passwords and other types of authentication credentials that **Company X** employees, contractors and third parties use for remote access capabilities must different from the passwords and other authentication credentials for all the other types of systems, sites, applications, devices, etc., for which they use authentication credentials.

2.18 **Company X** contractors and third parties with remote access IDs and remote access technologies must be immediately deactivated when no longer needed to fulfill contractual requirements.

3. Using Personally Owned Devices

3.1 Any personally owned computing or digital storage devices (from this point forward referenced as bring your own device, or "BYOD") used to store, process or otherwise access **Company X** information assets must be approved by the appropriate **Company X** manager and in accordance with the ***Wireless Access Management Procedure.*** **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

3.2 An inventory of all BYOD computing and digital storage devices must be maintained and included in the **Company X** central directory.

3.3 All BYOD devices must have **Company X** approved applications loaded on them to accomplish remote lock, wipe, and locate capabilities, in addition to encrypting all **Company X** data, using approved anti-malware tools, implementing personal firewalls approved by **Company X**, and configured in accordance with **Company X** firewall standards.

3.4 All BYOD computing devices used for remote and mobile working purposes must have current malware protection installed and enabled to prevent infections by: computer viruses, worms, Trojan horses, spyware, ransomware, and other types of malicious software, in compliance with the **Company X** ***Protection from Malicious Software Policy***. **[NOTE: Your organization should follow your policy for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

3.5 All remote working personnel, and personnel using BYOD devices, must follow the **Company X Security Incident and Privacy Breach Response Policies [NOTE: Your organization should follow your policy for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]** and associated procedures when they experience malware, see hacking attempts, have computing devices stolen, or suspect a security incident and/or privacy breach has occurred, or is in the process of occurring.

3.6 All personnel using BYOD devices to access **Company X** business assets must follow all the **Company X** information security and privacy policies when using the devices.

3.7 All remote and mobile working **Company X** employees, contractors and third parties are responsible for backing up business data on their BYOD devices, and the associated storage devices, to the necessary **Company X** file server or other backup storage device, in compliance with the **Company X**

Business Continuity and Contingency Policies. **[NOTE: Your organization should follow your policy for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

3.8 All remote and mobile working **Company X** employees, contractors and third parties are responsible for knowing and following the **Company X** ***Business Continuity and Contingency Policies*** **[NOTE: Your organization should follow your policy for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]** and following them in the event of a security incident or privacy breach that occurs in their remote work areas, and while they are doing work from mobile and BYOD devices.

4. Physical Security

4.1 When outside of **Company X** facilities, reasonable precautions must be taken to protect **Company X** hardware, software, and information from theft, damage, and misuse. Such precautions include, but are not limited to, the following:

1. Employees, contractors or third parties must not put laptops or mobile devices in checked luggage. These items must remain in personal possession at all times while traveling.
2. Mobile computers, storage devices, and confidential print material must be physically secured within hotel safes or other locked areas when such items are left behind in hotel rooms.
3. Mobile computers and storage devices must never be left in unattended cars, public accesses, unattended public venues such as restaurants or any other location where others could access or steal the devices.
4. Employees, contractors and third parties must take appropriate precautions when talking on phones, and other types of audible communications tools, involving conversations about confidential information, particularly in public or open places.
5. Home offices must be secured so that no others in the home have access to **Company X** information or physical assets.

4.2 In the event that a computing or storage device belonging to **Company X**, or a BYOD or other device, containing **Company X** information, is lost or stolen, or any other form of confidential information or personal information is lost or stolen, the **Company X** employee, contractor or third party involved with the loss or theft must follow the ***Security Incident and Privacy Breach Response Procedure***. **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

4.3 All **Company X** owned and BYOD computers, storage devices and information in all forms used for **Company X** business, are subject to being audited or inspected at any time by authorized **Company X** employees, contractors and third parties.

4.4 All **Company X** owned computing devices, mobile storage devices and information must be returned to **Company X** when **Company X** no longer employs employees, contractors and third parties.

4.5 Mobile and remote workers must not allow others to use their computing devices that have remote access capabilities to **Company X** networks and systems.

4.6 **Company X** employees, contractors and third parties must not share with others the computing devices and storage media they use for business purposes. If this cannot be avoided (getting a device repaired or serviced, a family member must use in an emergency, etc.) employees, contractors and third parties must ensure all computing device security settings and tools required by **Company X** are implemented.

4.7 **Company X** employees, contractors and third parties must thoroughly physically clean the surfaces of the device before using when it is returned, in accordance with the **Company X *Physical Safety Policies***. **[NOTE: Many organizations started implementing device cleaning policies with the advent of the COVID-19 pandemic. Change the title of the policy to your company's policy title. Or, if you don't have such an organizational policy, consider rewording this policy to establish one, or delete the last sentence in this policy statement.]**

5. Mobile Devices and Remote Access Security

5.1 Remote access into **Company X** networks and systems, and the use of mobile computing devices, will only be allowed using computing devices in accordance with the ***Wireless Access Management Procedure***. **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

5.2 **Company X** employees, contractors and third parties must strongly encrypt data on, sent from, and collected by, mobile computing and storage devices in accordance with the ***Encryption and Cryptography Use and Controls Procedure***. **[NOTE: Your organization should follow your existing procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

5.3 **Company X** employees, contractors and third parties must log out of and turn off mobile computing devices, BYOD devices and computing devices used in remote locations, when they are not using them.

5.4 **Company X** employees, contractors and third parties must follow the **Company X *Security Incident and Privacy Breach Response Procedure*** **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote and Mobile Computing Information Security & Privacy Policies document.]** when they experience a ransomware attack while remote computing, or using a mobile device.

5.5 When a mobile computing device, BYOD device, or digital storage device used for business activities or business data collection or storage is lost, stolen, or otherwise has fallen into untrusted hands and could be at risk of having the associated data accessed by an untrusted party, the data must be remotely deleted from the device in accordance with the ***Wireless Access Management Procedure.*** **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

5.6 Applications and data allowed on all mobile computing and storage devices used in any way for business purposes must be controlled and restricted in accordance with the ***Wireless Access Management Procedure.*** **[NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]**

6. Information and Systems Use

Information Asset Use

6.1 **Company X** provides information system resources in support of **Company X** remote and mobile business operations. **Company X** employees, contractors and third parties authorized to use **Company X** information systems may make incidental and occasional personal use of these systems when such use does not generate any additional costs to **Company X,** does not reduce **Company X** productivity or job performance, does not put information resources at risk, and is in compliance with all applicable laws, regulations, contractual requirements and policies.

6.2 **Company X** reserves the right to monitor all remote and mobile **Company X** employee, contractor and third-party activities that occur on **Company X** provided mobile computing devices and telephone systems, and BYOD devices, used for business purposes.

6.3 **Company X** reserves the right to monitor all **Company X** employee, contractor and third-party activity that occurs on employee-owned or other non-company-owned computing devices and telephone systems used for business purposes.

6.4 All voice and electronic communications and stored information created, transmitted, received, or archived in employee-owned or other non-company-owned computing devices and telephone systems used for business purposes are the property of **Company X**. **Company X** reserves the right to access and disclose all messages sent or received by email, instant messaging (IM), chat, app, social media and voicemail, in accordance with the **Company X *Mobile Working Approval Procedure***.

6.5 **Company X** employees, contractors and third parties must safeguard information while handling, processing, storing and sending in electronic and hardcopy communications while working remotely and/or using mobile computing devices. The safeguards must be consistent with the associated classification for that information. This policy applies to information in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of facsimile machines and any other sensitive items, such as blank checks and invoices.

6.6 **Company X** employees, contractors and third parties must use approved and **Company X**-supported electronic signature tools, in compliance with the **Company X *Electronic Signature Policy,* [NOTE: Your organization should follow your procedures for these activities; it is not part of this Remote Working and Mobile Computing Device Information Security & Privacy Policies document.]** for communications used to

remotely provide signatures in the place of handwritten signatures on hardcopies, digital forms, internet sites, and other types of forms and documents that require signatures that can be legally defensible and/or are required to support legal requirements. Refer to the **Company X** ***Electronic Signature Policy*** for the requirements and more information.

Software and Hardware Use

6.7 **Company X** must maintain a list of approved software and hardware to use for remote and mobile working, in accordance with the **Remote and Mobile Computing Software and Hardware Use Procedure**. Employees may only use such approved software and hardware for remote and mobile computing, on any device (whether owned by **Company X**, the employee, or someone else) used for remote and mobile computing.

6.8 Only those applications that are approved by **Company X** and that are properly licensed may be installed on employee-owned computing devices used for business activities, and **Company X** mobile computing devices.

Accessing and Posting to Public Sites

6.9 **Company X** employees, contractors and third parties must not post information about co-workers, customers, patients, consumers or others to online social media sites such as, but not limited to: Twitter, Facebook, LinkedIn, Google Docs, YouTube, Instagram, SharePoint, WhatsApp, Tik Tok, and others. This information must not be posted when away from **Company X** facilities from either **Company X**-owned computer equipment or equipment that is not owned by **Company X**.

6.10 **Company X** employees, contractors and third parties must be careful when posting to social media sites from remote home offices or other remove areas to ensure information is not inadvertently included in posts that show business information, includes audio from business discussions or events, and does not in some other way include any business information within the posts.

Remote Meeting Tools

6.11 Remote and mobile online meetings should be held only as authorized by **Company X Information Security, management, or whatever the most appropriate area/position is within your organization.**

6.12 All online remote working meeting tools (e.g., Zoom, Skype, GoToMeeting, Google Hangouts, join.me, etc.) must be approved by **Company X Information Security, management, or whatever the most**

appropriate area/position is within your organization prior to implementation and use.

6.13 Remote and online meeting tools must be kept patched and updated as soon as possible after new code is released in accordance with the ***Remote and Mobile Computing Software and Hardware Use Procedure***.

6.14 All "smart" Internet of Things (IoT) devices used outside of **Company X** facilities in support of online and remote meetings must be used in accordance with the **Company X** ***Remote and Mobile Computing IoT Device Use Procedure*** to prevent work activities from being recorded or captured.

Procedures Referenced from This Policy

- Mobile Working Approval Procedure
- Secured Area Access Procedure
- Work Area Security and Privacy Review Procedure
- Mobile Working Tracking Procedure
- Wireless Access Management Procedure **← Use your company's procedure for this**
- Security Incident and Privacy Breach Response Procedure **← Use your company's procedure for this**
- Encryption and Cryptography Use and Controls Procedure **← Use your company's procedure for this**
- Remote and Mobile Computing Software and Hardware Use Procedure
- Remote and Mobile Computing IoT Device Use Procedure
- Electronic Data Storage Device Disposal Procedure **← Use your company's procedure for this**
- Computing Device Disposal Procedure **← Use your company's procedure for this**
- Hard Copy information Disposal Procedure. **← Use your company's procedure for this**

Regulations and/or Standards Related to This Policy

A few of the standards, regulations and laws that these policies support and map to include:

- EU General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- California Consumer Privacy Act (CCPA)
- NIST Cyber Security Framework v1.1
- ISO/IEC 27001
- ISO/IEC 27002
- NIST SP 800-124 rev 1: Guidelines for Managing and Securing Mobile Devices in the Enterprise

Resources to Support Requirements in this Policy

See the information from Privacy Security Brainiacs on https://privacysecuritybrainiacs.com/free-resources/remote-working/ for information to support the policies above, as well as for supporting procedures, standards, tools, etc. Information will be added to this site periodically over time, so check back often, or sign up to get notices when new documents and tools are available.