**Team Briefing Agenda   
and Holiday Preparedness Checklist**

Use the following list as a template for your team briefing and for creating a customized checklist.

Need cybersecurity assistance? Email [help@501Secure.org](mailto:help@501Secure.org).

Questions about our services and program? Contact Kai Dailey, Program Manager at kai@501Secure.org



**Holiday Preparedness Checklist**

Please complete these steps before you leave on holiday.

**1. Secure Your Accounts**

Turn on Multi-factor Authentication (MFA) for all cloud applications. *[List specific websites and apps that your team uses.]* If a password is stolen, MFA significantly reduces the risk of unauthorized entry. *[If your organization has a policy requiring the use of passkeys or authentication apps rather than text or email, you can add that here.]*

* Watch out for Unexpected Codes. If you receive a text message, email, or notification from your authentication app asking you to approve a login and you are not currently attempting to log in, DO NOT APPROVE IT. Simply ignore or deny it, as this means someone else is trying to get into your account.
* Change weak passwords. Use a minimum 16-character, memorable phrase (e.g., Ocean-Downtime-Family-1020+Together).

**2. Secure Apps and Devices**

Before shutting down your laptop, log completely out of all websites and apps.

As an extra step, clear your web browser's cache and history. This removes any saved pieces of data that criminals could potentially access or use to get into your accounts.

Fully Shut Down your work laptop when not in use (don't just close the lid!) and store it safely in a locked drawer or office, out of sight. A powered-off device is the safest possible device.

**3. Protect Organization Data**

Do not email work files to your personal email "just in case." Work data must stay on secured work systems. If you will be working from home during your holiday break, move work files to approved cloud storage locations. *[List locations acceptable file store locations your organization uses e.g., OneDrive, Google Workspace, etc.]*

**4. Set up your Out-of-Office message with care.**

Do not provide details criminals can use to craft credible phishing emails that appear to come from within your organization. Use the same caution with social media posts.

**5. Emergency Preparedness**

For any urgent after-hours communications, your single point of contact is *[Name of Manager/Designated Person]* via *[Designated Contact Method, e.g., personal cell phone or specific external email]*.

**6. Verify Unexpected Messages (Watch for Social Engineering and Scams!):**

* + Fake IT/Help Desk Warnings: Ignore unexpected calls, pop-ups, or emails claiming your computer has a problem and asking you to call a number or allow remote access. Legitimate tech support will never contact you out of the blue to fix a non-reported problem.
  + Click-Fix Scams: Never follow instructions from a website or pop-up that tells you to copy and paste code into your computer's Run box, Terminal, or Command Prompt to fix an error. This is a common tactic to trick you into installing malware yourself.
  + Financial Fraud: Any unexpected request for purchasing gift cards, performing an emergency wire transfer, or immediate payment of an invoice (that bypasses standard procedure) is a scam. Always verify using the Designated Emergency Contact method above.

**7. Offline Emergency Plan**

Please ensure you have a copy of our Business Continuity/Emergency Response Plan available offline (e.g., a printed copy or a saved PDF on your personal device) in case our systems are completely unavailable.