|  | **TASK** |
| --- | --- |
|  | 1. **Enforce a Strong Password Policy**    * Establish the password complexity    * Unique password for every work account    * Regular password updates (Expiration policy: \_\_\_ months)    * Install a password manager |
|  | 1. **Update Your System Regularly**    * Update the operating system for desktop and mobile devices    * Enable automatic updates    * Schedule maintenance updates |
|  | 1. **Find a Secure VoIP Provider**   Look for the following security features:   * + End-to-end encryption   + Single sign-on   + Multi-factor authentication   + Compliance standards |
|  | 1. **Disable International Calling**    * Configure calling permissions    * Restrict international dialing patterns    * Enable geofencing    * Review call activity |
|  | 1. **Disable Web Interface Use**    * Identify critical users    * Disable web access    * Restrict IP address    * Configure role-based access controls    * Monitor log access |
|  | 1. **Conduct Security Audits**    * Select a reputable third-party agency    * Gather required documentation    * Implement recommendations    * Schedule a follow-up audit |
|  | 1. **Install VPN Software**    * Evaluate VPN requirements    * Select a VPN provider    * Configure VPN (protocol selection)    * Deploy VPN software to remote staff    * Monitor VPN activity |
|  | 1. **Monitor Call Logs**    * Identify key indicators (e.g., call patterns, duration, & caller IDs)    * Set threshold alerts    * Restrict call log access    * Implement regular call log review |
|  | 1. **Set Up Firewalls**    * Select a firewall software provider    * Configure firewall settings    * Update firewall software |
|  | **10. Train Staff on Cybersecurity**   * + Develop training materials   + Conduct training sessions on common threats & best practices   + Create hands-on training and simulations   + Promote ongoing awareness |