PAKISTAN BANKS’ ASSOCIATION

WORK FROM HOME

Guidelines developed by PBA Cyber Security Forum

REMOTE WORKING

Remote working is a work arrangement which allows employees to work outside the traditional office environment. It is based on the concept that work does not need to be done in a specific place to be executed successfully

CYBER SECURITY RISK

Remote working, whilst providing many opportunities, can also present organisations with a number of cyber security risks, including:

- Data leakage
- Malicious attacks from threat actors
- Non-approved Bank technology

Depending on the severity of the incident involved, the consequences of data leakage or a malicious attack from threat actors can cost the Bank:

- Adverse publicity and reputational damage
- Financial loss (if the Bank has to notify and compensate those affected)
- Regulatory fines

END USER SECURITY

Home WIFI (Router) secure configuration:

- Network Encryption**:** Set the strongest network encryption that is compatible with your device so that any wireless device seeking connection will require the key.

    a. To enable security, open your router setup screen and look for a Wireless Security section
    b. Select the wireless security method of either WPA or WPA 2. WPA 2 is the RECOMMENDED encryption method

- WPA and WPA 2 are more secure and offer greater protection against hacking and security breaches. WEP does not protect networks against a determined hacker. If your router only supports WEP, upgrade to a newer device.

a. Change the default router password. Enter the passphrase which should comply with Leading Password practices (8 characters, upper and lower case, numbers and special characters)
b. You should not use your official Password. This passphrase will need to be entered into every device you use to connect to your home wireless network.

- Change the default SSID (Service Set Identifier) name. The SSID is the name that identifies your wireless router. When naming the router, do not use your family or any other identifiable information.

- Disable SSID Broadcast. Note that when disabling the SSID broadcast, it will require that you manually enter your unique SSID when wanting to connect any new device to your wireless router. To help make finding your wireless network easier, wireless routers broadcast your SSID, which means anyone looking for a wireless router could see your SSID. Disabling the SSID broadcast feature make it more difficult for someone to find your network when browsing available wireless networks.

Recommendation: Position router near the centre of the home rather than near windows to minimise leakage. Turn off your wireless network during extended periods of non-use.

Your system may have been compromised if:

a. Your system is slower than normal
b. Additional popup windows or dialog boxes show up (which may appear and disappear quickly)
c. Your web browser has new toolbars, the search engine has changed or the home page is different
d. There are new icons on the desktop
e. Your camera light is on when you are not specifically using it
f. Files are missing
g. Your mouse cursor moves by itself

- If you suspect your system is compromised, isolate the system from network and other devices and seek professional advice and help.

- Backup data on a regular basis. Beware; backups can be compromised too. Consider authorised services for off-site backup as well.

- Handle bank Information via bank provided computers or Mobile Devices or those that are covered under bank Policies.

- Avoid connecting to unknown Wi-Fi networks, use multi-factor authentication and connect with the right corporate VPN gateway.

- Do not leave your corporate laptop, mobile, tablets in unsecure locations (e.g. unattended in public, in your car, etc).

- Be aware of your surroundings. Information may be leaked through shoulder surfing and eavesdropping especially in public.

- Use appropriate information classification while saving and sharing information inside/outside of the bank.

- Check the real destination of the links sent in emails by hovering mouse over the link. Be cautious when clicking on external meeting links. Do not open, forward or respond to emails from unrecognised email addresses.

- Prohibit working from public places, such as coffee shops or on public transportation, where third parties can view screens and printed documents.

- Online Meeting & Calls:
  a) Mute the microphone when not speaking in a conference call.
  b) Webcams should be blocked by default unless required in a meeting.

- Change your password regularly. Do not reuse passwords for multiple accounts.

- Never disclose your password to anyone. Longer passwords are harder to guess. Where possible use a password, which is 8 characters or longer.

- Ensure that your device has antivirus installed and that it is set to scan all files and folders on the devices regularly. Ensure that automatic update is turned on so that the anti-virus is always aware of the latest threats.

- If you have to share information with the authorised party, send it to them via email. Ensure that you use appropriate information classification and data encryption methods for all files that you share.

- Avoid using your work email address to sign up for any external accounts online, unless authorised for work.

- Stay alert against phishing attempts. Falling prey to a phishing attack can lead to data breaches and/or ransomware attacks that can compromise the Bank's network.

- Secure all printed work material, even at home. Do not take classified information outside of the Bank's workspace. Users must not disclose any sensitive business information outside Bank.

- Avoid connecting any other type of USB devices into your computer besides your mouse, headset and your phone in the specific port designated for charging it.

- Ensure you regularly restart your laptop/desktop. This will facilitate mandatory security updates that will help keep your information safe.

- Don’t remain connected to the VPN constantly – work offline whenever not required for teleworking. Users are also advised to lock their laptops / systems / mobiles and log out active sessions when they are not in use.

- Don't use collaboration tools which are not approved or issued by the Bank e.g. Don't host calls or converse on work-related matters via your personal Teams account, Facebook video, FaceTime, WeChat, WhatsApp or similar. These can pose security risks to the Bank. However, you may use these tools to join a call as a guest using the web browser, in the case you receive an invite from a credible third party such as a client, vendor or regulator.

- Limit the administrator accounts to staff who do not use these accounts for emails, video streaming and web browsing etc.

- Any loss / theft /damage of Bank provided laptops shall be reported to Incident Management Team on immediate basis. Incident management team shall take immediate corrective actions as per need and requirement of the incident.

NETWORK SECURITY

- **VPN Connection with Multi Factor Authentication:** To keep banks’ critical information secure, considering deploying MFA Control. It allows to connect to the Bank’s resources more securely whilst working remotely.

- Map out the network centric border security controls that apply to machines when they are on the internal network and evaluate whether a similar control set still applies to network traffic from these systems when not on the internal network.

- Secure web browsing with web filtering / web security gateway when working remotely and if not, consider deploying web filtering solution to detect and prevent malicious web traffic. Configure web filtering solution to restrict the types of websites that can be accessed, restrict file types users can download and block access to newly registered or untrusted domains.

SYSTEMS AND INFRASTRUCTURE SECURITY

- Regular patch management is done to fix any security vulnerability where applicable.

- Perform OS hardening based on best practices and system policies, removing unnecessary applications and services to minimize the OS exposure to threats and to mitigate potential risks.

- Block access to external media including but not limited USB (mass storage devices), CD/DVDs etc.

- Performing regular infrastructure assets scanning to govern and report the compliance status of the assets.

- Protect internally hosted instant messaging infrastructure by:
  a. Preventing use of public instant messaging applications that are not authorised
  b. Employing a standard client configuration for the instant messaging applications
  c. Hardening instant messaging servers
  d. Configuring firewalls to block unauthorized instant messaging traffic.
  e. Disabling unauthorised features such as file sharing, audio and video files
  f. Directing messages through a content filter
  g. Using encryption
  h. Enable malware scanning where applicable
  i. Logging important events

- Consider applying key security controls including full disk encryption, anti-malware protection, data loss prevention, automated backup solutions, endpoint detection and response tools to laptops provided for remote connectivity.

ACCESS MANAGEMENT

- Use privileged access management solutions for securing and segregating privileged access to prevent attackers from compromising high value accounts and the wider network.

- Regular review of user access to applications/services and align accesses as per job roles.

- Remote working access is based on formal process that at minimum requires Line Manager and concerned management approval. However remote access is implemented with principles of ‘Least Privilege’ and ‘Need-to-Know-based Access Control’ in line with international standards and best practices.

- Sharing of work computers and other devices is prohibited. When employees bring work devices home, those devices should not be shared with or used by anyone else in the home. This reduces the risk of unauthorized or inadvertent access to protected company information.

BUSINESS RESILIENCE

- Monitor the IT help desk to identify complaints from employees about processes, controls or technology limitations that are preventing them from working remotely.

INFORMATION AND CYBER SECURITY

- Confirm tools related to Data Leakage and other security controls on laptops perform as expected when devices are removed from the internal network for extended period of time.

- Monitor leakages of sensitive information through DLP controls deployed at various end points.

- Consider implementation of Mobile Device Management (MDM) solutions that enables bank to secure and enforce policies for mobile devices and tablets, allowing them to securely access banks' data and resources.

- Monitor Endpoints through Endpoint protection and Endpoint detection and response solutions deployed as part of bank's cyber security efforts.

- Review all remote access systems to ensure critical security patches have been applied and secure configurations have been used.

- Implement stringent controls for third party service providers and connections. Should any third parties fail to demonstrate adequate security controls and procedures, consider limiting or even suspending their connectivity until they remediate their weaknesses.

- Configure remote access solutions, email systems and Active Directory to log all authentication events. Preserve logs and analyse these for anomalous activity, including brute force attempts, logins from unfamiliar locations, and logins that indicate impossible travel.

- Organise a short 'working from home' security awareness module to help the workforce understand the potential threats and safeguards they may need to take when working remotely If not, try creating a short fact sheet or guidance note. A periodic security awareness program for remote users should also be part of the organization's awareness drive.

- Analyse that teams have the people, processes and technology necessary to monitor and respond to alerts, with appropriate levels of redundancy. Consider augmenting Security Operations teams with SIEM and related resources.
- Information Security teams should work with IT to understand the resilience of remote access systems to DDOS attacks, including reviewing bandwidth available, limitations of remote access software and whether any DDOS protection services can be added in front of them.
- As VPN is most critical in WFH scenario, the following use cases are recommended for monitoring where possible.
  - Abnormal VPN connections from the user
  - Abnormal VPN session duration
  - First VPN connection from an unknown device
  - VPN connection from an anonymous proxy
  - Abnormal amount of data uploaded during a VPN session
  - Increase of company-related data files access
  - MFA from a new device for a user
  - Too many failed VPN logins
  - VPN access from a disabled account
  - Source IP from unauthorized location
  - Malicious VPN source IP