PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

(2026 – 27)

A practical handbook for government and public-sector cybersecurity awareness

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

DISCLAIMER

This handbook is produced and published by the National Cyber Emergency Response Team of Pakistan (PKCERT), Government of Pakistan.

The policies, controls, and safe practices outlined herein are prescribed in accordance with local national laws, statutory regulations, and international cybersecurity best practices.

The contents of this document serve as the baseline operational standard for digital security across public sector entities.

While these guidelines are designed to mitigate cyber risks significantly, adherence to this handbook does not guarantee complete immunity from sophisticated cyber threats. Departmental IT or Cybersecurity teams must continuously monitor, update, and enforce technical security controls alongside user awareness.

About this Handbook

The National Cybersecurity Handbook is a practical guide developed to help employees, officers, officials, and technical personnel across the Federal Government, Provincial Governments, and Public Sector Organizations of Pakistan towards adopting secure cyber practices in their day-to-day work.

As government services become increasingly digital and interconnected, the actions of every user directly influence the confidentiality, integrity, and availability of national information assets. Cybersecurity is therefore not solely a technical function, but a shared responsibility of every government employee. This handbook translates the requirements of the Pakistan Information Security Framework (PISF) 2026, the National Cyber Security Policy 2021, the CERT Rules 2023, and other applicable national laws, regulations, and government directives into clear, practical guidance that can be readily applied in everyday operations. It also incorporates internationally recognized cybersecurity standards and best practices to promote a consistent, risk-based approach to protecting government information and systems.

Organized into eight practical domains, the handbook provides concise guidance, recommended practices, and user responsibilities to help government personnel prevent cyber incidents, protect sensitive information, support regulatory compliance, and strengthen Pakistan's overall cyber resilience.

PKCERT

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

National Cybersecurity Handbook

The National Cybersecurity Handbook consolidates mandatory cybersecurity guidelines into eight practical domains to facilitate consistent implementation, awareness, and day-to-day reference.

1. **Secure Use of Official Email**
2. **Device Security**
3. **Password Security**
4. **Data Security**
5. **Internet Security**
6. **Secure Use of Removable Media**
7. **Secure Remote Access**
8. **Incident Response**

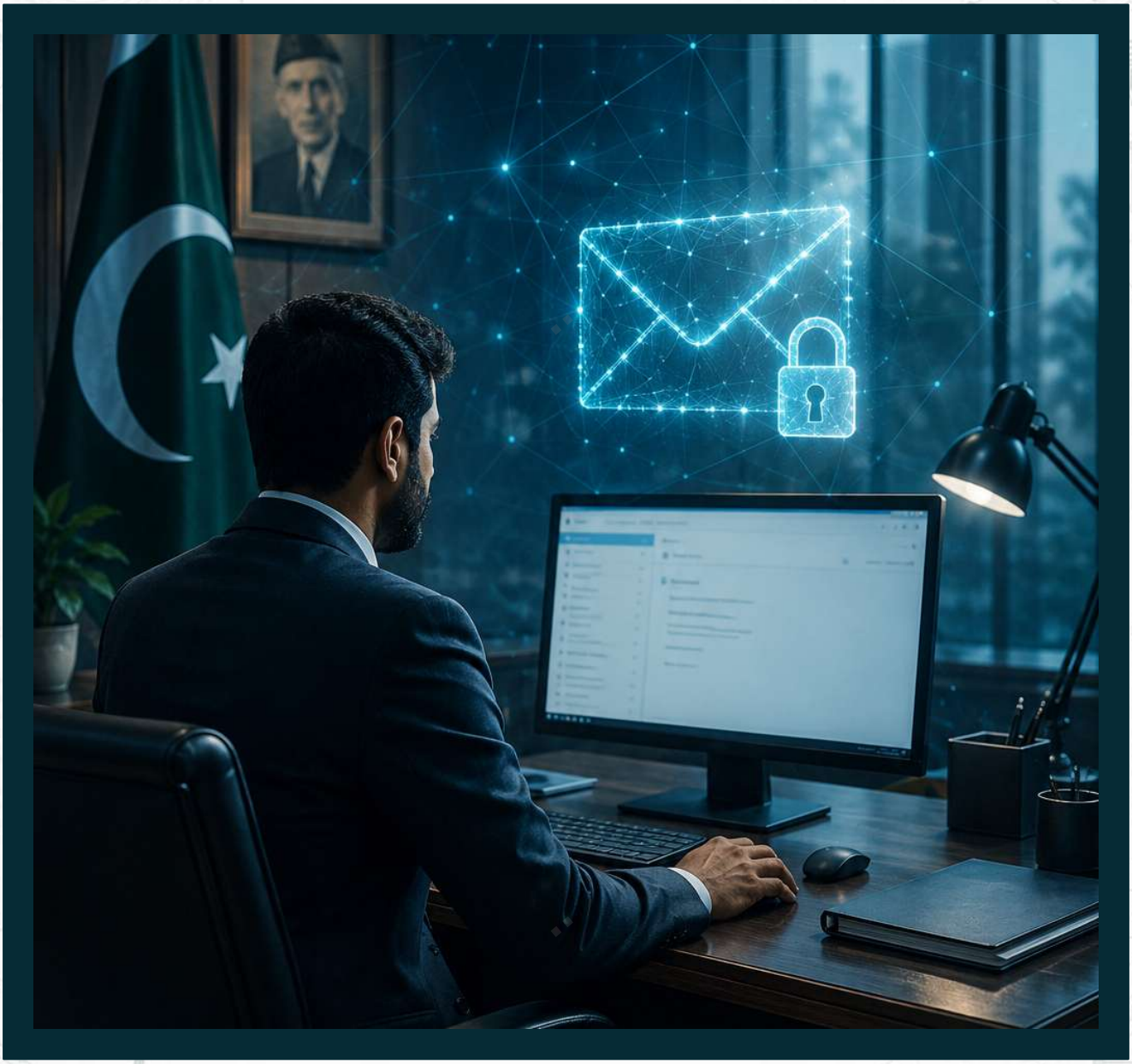
Readers should keep the National Cybersecurity Handbook accessible at their workstations and consult relevant domains before starting new tasks. Departmental supervisors and IT or Cybersecurity teams should use these guidelines as baseline checklists for internal audits and team trainings.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook



Secure Use of Official Email

Guidelines for Secure and Responsible Use of Official Email

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Conduct official email communication only through your official email account.

1

تمام سرکاری مراسلت صرف سرکاری ای میل اکاؤنٹ کے ذریعے انجام دیں۔

Official email accounts provided by the Government of Pakistan are trusted channels for conducting official correspondence.

Un-official email accounts must not be used unless expressly authorized by the concerned department as a special arrangement under exceptional circumstances.

DO's

1. **Use your official email account for all official correspondence and departmental tasks.**
2. **Share your official email address only with trusted entities.**
3. **Review your email account activity regularly and report any suspicious activity to your IT or Cybersecurity team.**
4. **Keep your email security settings up to date. Contact your IT or Cybersecurity team for assistance with security configurations.**

DON'Ts

1. **Do not use personal email accounts (like Gmail or Yahoo) to conduct official correspondence.**
2. **Do not register your official email address on shopping, gaming, or social media sites.**
3. **Do not send/forward emails from your official government email to your personal inbox.**
4. **Do not share departmental mailing lists or official email directories with unauthorized entities.**

RISKS OF NON-COMPLIANCE

- **Exposure of sensitive government data to unauthorized entities**
- **Increased risk of phishing & email spoofing**
- **Account compromise and unauthorized use of email accounts**

In **Email Spoofing** attack, the attacker sends a fake email that appears to come from a trusted government organization, to deceive recipients into giving up sensitive data, transferring funds, or downloading malicious files.

Always verify incoming emails before responding, clicking on links or sharing sensitive information.

2

کسی بھی موصول ہونے والی ای میل کا جواب دینے، اس میں موجود لنکس پر کلک کرنے یا حساس معلومات شیئر کرنے سے پہلے ہمیشہ اس کی تصدیق کریں۔

Always verify the sender's identity, email address, links, attachments, and requests before responding, clicking on links or sharing sensitive information.

Be cautious of urgent warnings, unexpected prizes, password-reset messages, and requests for login credentials or financial details.

DO's

1. **Inspect the full email header to verify that the address after @ symbol matches the official organizational domain.**
2. **Hover over embedded links to inspect the full destination URL before clicking on them.**
3. **Verify suspicious requests out-of-band (via official phone call or in-person visit) before taking action or sharing sensitive details.**
4. **Report unverified or suspicious emails immediately to your IT or Cybersecurity team using official channels.**

DON'Ts

1. **Do not click on unexpected links or open attachments from unknown, unverified, or suspicious senders.**
2. **Do not respond to urgent demands for data, credentials, or immediate funds transfers without proper verification.**
3. **Do not enter login credentials or sensitive details through unverified links or forms included within incoming emails.**
4. **Do not forward suspicious emails to internal or external recipients without explicit guidance from your IT or Cybersecurity team.**

RISKS OF NON-COMPLIANCE

- **Exposure of government infrastructure to malware infections**
- **Theft or leakage of sensitive data and administrative credentials**
- **Disruption in public services and loss of public trust**

Email Header is the hidden "digital envelope" of an email. While you usually only see the sender's display name, the header contains underlying technical details such as the true sending server, exact email address, and security verification checks, that reveal where the email actually came from.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

Device Security

Guidelines for Secure Use of Devices for a Safer Digital Environment

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Use authorized devices for performing official work.

3

سرکاری کام منظور شدہ آلات پر انجام دیں۔

Official devices issued by the Government of Pakistan are configured with mandatory security controls and security software. Therefore, official work should be performed using official devices.

Where government-issued official devices are not available and the use of personal devices becomes operationally necessary, you should obtain prior authorization from your concerned department before using personal devices for official work.

DO's

1. **Use official devices (computers, laptops, tablets, phones, etc.) for performing official tasks.**
2. **Obtain prior approval from your concerned department before using personal devices for official purposes.**
3. **Ensure that any personal device approved for official use meets the required security standards.**
4. **Immediately report any loss, theft, or suspected compromise of a device to your concerned department.**

DON'Ts

1. **Do not use unauthorized personal devices for official work.**
2. **Do not access sensitive applications like e-Office or other classified government web portals on personal devices.**
3. **Do not allow unauthorized individuals (including friends and family members) to use official devices.**
4. **Do not connect personal storage devices (USBs or Hard Drives) or your personal phones to official devices.**

RISKS OF NON-COMPLIANCE

- **Leakage of government data through unprotected personal devices**
- **Increased risk of malware spread through personal devices**
- **Loss of audit traceability during cyber incident investigations**

The term **Shadow IT** is used to refer to any hardware device, software application, or digital tool used for official work without prior approval or authorization from the concerned department. Shadow IT creates security blind spots that attackers exploit to breach government networks.

Keep devices secure by following security guidelines and managing user controls.

4

آلات کی حفاظت کے لیے سیکیورٹی ہدایات اور بنیادی اصولوں پر عمل کریں۔

Users must practice user-level security controls including strong PINs and passwords, screen locking, and overall physical security of their devices.

To maintain good device hygiene, users should promptly cooperate with their IT or Cybersecurity team when operating system updates and security patches are scheduled for their devices..

DO's

1. **Always lock your device screen when leaving your desk.**
2. **Set strong, complex passwords or PINs on all computers, phones, laptops, and tablets used for official work.**
3. **Contact your IT or Cybersecurity team if you observe any unfamiliar prompts on your device screen.**
4. **Follow security directives, advisories, and instructions issued by your IT or Cybersecurity team.**

DON'Ts

1. **Do not leave your device unlocked while away from your desk or exposed to physical shoulder-surfing.**
2. **Do not attempt to disable security settings, uninstall security software or modify system configurations on your device.**
3. **Do not share login credentials, access PINs, or screen lock patterns with anyone including colleagues.**
4. **Do not take official devices outside the workplace unless required for official duties.**

RISKS OF NON-COMPLIANCE

- **Unauthorized physical access to sensitive government data**
- **System instability due to missing updates and patches**
- **Compromised accountability caused by shared passwords**

Shoulder Surfing is when someone standing near you or behind you obtains your passwords, PIN or data by secretly watching, as you type this information using your device keypad or keyboard.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

Password Security

Guidelines for Creating, Managing, and Protecting Passwords

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Use strong, unique passwords or passphrases for official accounts and applications.

5

سرکاری اکاؤنٹس اور ایپلیکیشنز کے لیے مضبوط اور منفرد پاس ورڈز یا پاس فریزز استعمال کریں۔

Passwords serve as the primary defensive barrier against automated brute-force attempts and unauthorized system access.

Therefore, users should set strong, complex and unique passwords for their accounts.

DO's

1. **Use long passphrases combining uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols (!@#$).**
2. **Set distinct, unique passwords for each application or account.**
3. **Enable Multi-Factor Authentication (MFA) on official portals and applications to add an extra layer of security.**
4. **Frequently change passwords and passphrases.**

DON'Ts

1. **Do not reuse passwords across personal and government accounts, or multiple official platforms/applications.**
2. **Do not include predictable personal details like your name, date of birth, or dictionary words (e.g. Password123).**
3. **Do not write passwords on physical sticky notes, or share them with colleagues.**
4. **Do not save official passwords in unmanaged browser auto-fill on shared computers.**

RISKS OF NON-COMPLIANCE

- **Account takeover and unauthorized use of official accounts**
- **Official identity theft**
- **Exposure of official files and correspondence**

In a **Brute Force Attack,** an attacker uses automated tools to repeatedly guess passwords until the correct one is found. **Multi-Factor Authentication** adds an extra verification step through use of OTP or biometric verification to prevent the attacker from accessing the account only with a password and without the second factor.

Ensure secure storage, management, and handling of official login credentials.

6

سرکاری لاگ اِن معلومات کی محفوظ ذخیرہ کاری، انتظام اور استعمال کو یقینی بنائیں۔

Access credentials, passwords, and passphrases are the keys to official networks.

Securing how passwords and sensitive authentication data are stored, shared, and managed prevents unauthorized access and lateral movement across systems..

DO's

1. **Store official credentials only in officially approved, encrypted password vaults.**
2. **Always double-check the URL and SSL certificate before typing login details into any web application.**
3. **Immediately notify your IT or Cybersecurity team if you suspect your password has been leaked.**
4. **Keep administrative/privileged login credentials strictly separate from daily work accounts.**

DON'Ts

1. **Do not store credentials in unencrypted spreadsheets, text files, or emails.**
2. **Do not share your official credentials or MFA security tokens/codes with anyone.**
3. **Do not approve push notifications or login requests that you did not initiate yourself.**
4. **Do not use unknown or unauthorized authenticator apps from untrusted sources.**

RISKS OF NON-COMPLIANCE

- **Exploitation of admin rights causing full system compromise**
- **Exposure of operational accounts across breach databases**
- **Unauthorized network lateral movement**

In a **Credential Harvesting** attack, adversaries use fake login pages (phishing) to trick users into revealing usernames and passwords. When MFA is enabled, attackers may use **MFA Fatigue** (**Push Spamming**) by sending repeated login prompts until the user accidentally approves access. Always verify the source of every authentication prompt before accepting.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

Data Security

Guidelines for Ensuring Security of Government Data

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Classify official data before storing, sending or sharing it.

7

سرکاری ڈیٹا محفوظ کرنے یا شیئر کرنے سے پہلے اس کی درجہ بندی کریں۔

Data classification is the process of categorizing information based on its sensitivity, importance, and required level of protection.

All official data must be classified according to a department's approved data classification scheme and aligned with the Pakistan Information Security Framework (PISF) to ensure appropriate handling, access control, and protection.

DO's

1. **Classify all official data according to the approved departmental data classification scheme and PISF requirements.**
2. **Understand the sensitivity level of the data you create, receive, or handle.**
3. **Apply appropriate classification labels to documents, files, and records.**
4. **Consult the relevant authority, or your IT or Cybersecurity team when the classification requirements are unclear.**

DON'Ts

1. **Do not handle official information without knowing its classification level.**
2. **Do not downgrade or change the classification level of a data asset without authorization.**
3. **Do not leave classified sensitive documents visible on desks or in printer trays.**
4. **Do not disclose your department's data classification scheme to unauthorized individuals.**

RISKS OF NON-COMPLIANCE

- **Improper handling of sensitive government information**
- **Accidental disclosure of confidential data**
- **Failure to meet departmental data security and PISF requirements**

The **Pakistan Information Security Framework (PISF)**, issued by PKCERT, establishes mandatory baseline controls to protect sensitive and critical data. The framework mandates data security controls like classification, encryption, access control, governance, and data lifecycle management.

Apply appropriate security controls based on data classification level.

8

ڈیٹا کی درجہ بندی (کلاسیفکیشن) کے مطابق مناسب سیکیورٹی کنٹرولز کے استعمال کو یقینی بنائیں۔

Applying appropriate security controls based on data classification ensures that official information remains protected throughout its lifecycle.

Users must apply the required security measures defined for each classification level, including appropriate access, storage, sharing, and disposal controls.

DO's

1. **Apply security controls according to the assigned data classification level.**
2. **Share classified information only with authorized individuals on a need-to-know basis.**
3. **Store and transmit sensitive information using approved government systems and secure channels.**
4. **Follow your department's approved procedures for retention, archiving, and secure disposal of classified data.**

DON'Ts

1. **Do not share classified information through unauthorized email accounts, applications, or devices.**
2. **Do not store sensitive government information on personal devices or unapproved platforms.**
3. **Do not access classified information without proper authorization.**
4. **Do not dispose of classified information without following approved disposal procedures.**

RISKS OF NON-COMPLIANCE

- **Unauthorized access to sensitive government information**
- **Data leakage or compromise of official records**
- **Increased risk of cyber incidents and information misuse**

Data Handling refers to the way information is accessed, stored, shared, processed, and disposed of throughout its lifecycle. The required protection measures depend on the classification level of the data.

Backup critical official files on regular basis.

9

اہم سرکاری ڈیٹا کا باقاعدگی سے بیک اپ بنائیں۔

Storing critical data only on a single device exposes it to accidental loss due to hardware crashes, ransomware, and unauthorized deletion.

Therefore, government personnel must maintain routine backups on secure government infrastructure.

DO's

1. **Maintain backup copies of all critical documents on both local device and servers as provided by your IT team.**
2. **Set regular backup schedules (daily, weekly, or monthly) based on the importance of your data.**
3. **Contact your IT or Cybersecurity team to set up secure storage and encryption for your backups.**
4. **Regularly test your backups to ensure that data can be successfully restored.**

DON'Ts

1. **Do not store critical official data exclusively on a single PC or laptop without external backup.**
2. **Do not use unauthorized commercial cloud platforms or personal USB drives for back up of official data.**
3. **Do not delete old backups without following approved retention procedures of your department.**
4. **Do not store backups and original data in the same location, as both may be lost during an incident.**

RISKS OF NON-COMPLIANCE

- **Permanent loss of critical government data**
- **Extended operational failure and severe downtime**
- **Violation of national data protection mandates**

3-2-1 Backup Principle suggests that users should maintain three copies of their data, store them on two different types of storage, and keep one copy in a separate location. For example, keep the original file on your computer, one backup on external storage device or server, and another backup in a separate secure location or approved cloud service to ensure data can be recovered if one copy is lost or compromised.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

Internet Security

Guidelines for Secure Use of Internet and Web Resources

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Access only trusted websites and verify their authenticity before sharing any information or credentials.

10

صرف قابلِ اعتماد ویب سائٹس استعمال کریں اور معلومات یا اسناد درج کرنے سے پہلے ویب سائٹ کی تصدیق کریں۔

Unverified websites may pose security risks by stealing sensitive information, spreading harmful software, or redirecting users to fake websites.

Therefore, users should always verify website links, domain names, and login pages before entering any official information.

DO's

1. **Use saved bookmarks or manually enter official website addresses to access authorized portals securely.**
2. **Verify website addresses before signing in to ensure you are accessing the correct and authorized portal.**
3. **Download files only from verified and trusted websites.**
4. **Report suspicious websites, pop-ups or redirects immediately to your IT or Cybersecurity team.**

DON'Ts

1. **Do not click shortened or suspicious links without verification.**
2. **Do not ignore browser warnings or bypass blocking of unsafe websites.**
3. **Do not enter credentials on webpages reached through unknown links.**
4. **Do not download files, installers or browser extensions from untrusted websites.**

RISKS OF NON-COMPLIANCE

- **Credential theft through fake login pages**
- **Malware infection from unsafe downloads**
- **Unauthorized access to official services**

Attackers may create **Fake Login Pages** that closely resemble official websites. Always verify the website address, as even a minor change in the domain name can indicate a fraudulent website.

Connect only to authorized, encrypted network infrastructure and secure access points.

11

صرف مجاز اور محفوظ نیٹ ورک کنیکشنز اور اینکرپٹڈ وائی فائی کا استعمال کریں۔

Unsecured and rogue networks enable cyber attackers to intercept sensitive communications, perform Man-in-the-Middle (MitM) attacks, or inject malware.

Therefore, users must strictly adhere to network security controls and avoid unauthorized Wi-Fi or unverified network connections.

DO's

1. **Connect to internet only through official LAN (Ethernet) cable or secure and encrypted official Wi-Fi networks.**
2. **Disable "Auto-Connect" for Wi-Fi on mobile devices and laptops.**
3. **Verify official network SSIDs with your IT or cybersecurity team prior to establishing connection.**
4. **Report suspicious or unknown Wi-Fi connections to your IT or Cybersecurity team.**

DON'Ts

1. **Do not conduct official business or access sensitive information over open public Wi-Fi.**
2. **Do not connect unauthorized personal routers, hotspots, or rogue access points to official wall jacks.**
3. **Do not enable network discovery or file/folder sharing on untrusted non-official networks.**
4. **Do not bypass untrusted network security alerts or invalid SSL/TLS certificate warnings.**

RISKS OF NON-COMPLIANCE

- **Eavesdropping & Man-in-the-Middle (MitM) packet sniffing**
- **Rogue Access Point interception leading to session hijacking**
- **Cross-device malware infection through untrusted networks**

Attackers frequently create **Evil Twin / Rogue Wi-Fi Networks** that mimic official network SSIDs. Therefore, it is important to always verify network legitimacy before transmitting any sensitive data or logging into official portals.

Use only authorized cloud services and secure web and mobile applications.

12

سرکاری امور کے لیے صرف مجاز کلاؤڈ سروسز اور محفوظ ویب اور موبائل ایپلیکیشنز کا استعمال کریں۔

Unsanctioned cloud storage and untrusted web/mobile applications present severe risks of data leakage, regulatory non-compliance, and credential theft.

Users must not use web/mobile applications and cloud platforms that do not comply with Government of Pakistan's security standards.

DO's

1. **Use only officially sanctioned cloud services and web/mobile applications approved by your department.**
2. **Enforce Multi-Factor Authentication and Role-Based Access Controls (RBAC) on cloud portals.**
3. **Verify HTTPS, valid SSL/TLS certificates, and secure configurations before logging into web apps.**
4. **Classify data before uploading to cloud repositories to ensure compliance and privacy.**

DON'Ts

1. **Do not upload sensitive documents to personal cloud storage or unvetted AI tools.**
2. **Do not share administrative credentials, access tokens, or API keys across open chats.**
3. **Do not bypass Cloud Access Security Brokers (CASB) or proxy firewalls to access Shadow IT apps.**
4. **Do not store unencrypted passwords or API secret keys in public cloud repositories or code bases.**

RISKS OF NON-COMPLIANCE

- **Sensitive data spillage and intellectual property leakage**
- **Account takeover and unauthorized data modification**
- **Violation of national data sovereignty guidelines**

Cyber adversaries heavily exploit **Shadow IT & Unsanctioned Cloud Web Apps** to exfiltrate sensitive data. Always consult your IT or Cybersecurity team prior to adopting any new web portal or cloud service for official work.

Be careful when using social media and do not share official information.

13

سوشل میڈیا کے استعمال میں احتیاط برتیں اور سرکاری معلومات شیئر کرنے سے گریز کریں۔

Social media platforms (such as Instagram, Facebook, and X) are often targeted by attackers to gather information about individuals and organizations, and use it to launch phishing, social engineering, and other cyber attacks.

Therefore, government personnel must exercise extreme caution when using social media.

DO's

1. **Learn and follow your department's social media policies and guidelines.**
2. **Configure strict privacy settings and enable Multi-Factor Authentication (MFA) across all social platforms.**
3. **Maintain strict confidentiality for official data and keep personal social accounts separate from official work accounts.**
4. **Verify the identity of unknown profiles and report suspicious connection requests or messages to your IT or Cybersecurity team.**

DON'Ts

1. **Do not post photographs of official documents, workplace security badges, or restricted government premises.**
2. **Do not express personal opinions using official titles or organizational affiliations.**
3. **Do not accept unsolicited connection requests, click unknown links, or open attachments in direct messages.**
4. **Do not post classified information (like project details, internal policies, official travel schedules) on social media.**

RISKS OF NON-COMPLIANCE

- **Targeted spear-phishing and social engineering attacks**
- **Accidental exposure of sensitive documents and internal details**
- **Account hijacking used for impersonation or disinformation**

Your **Digital Shadow** is the information about you that exists online through your posts, profiles, interactions, and activities. Attackers may analyze this information to understand targets and identify opportunities for exploitation. The process in which attackers collect small pieces of publicly available information from different sources and combine them to build a detailed picture of their target, is called **Information Harvesting**.

Ensure safe and responsible use of Artificial Intelligence (AI) tools.

14

مصنوعی ذہانت (اے آئی) ٹولز اور جنریٹو ماڈلز کا محفوظ اور ذمہ دارانہ استعمال یقینی بنائیں۔

Submitting sensitive classified government data into public AI platforms poses severe risks of data leakage and unauthorized retention by AI tools.

Users must strictly follow official government guidelines when utilizing AI chatbots, research models, or automated writing assistants for daily tasks.

DO's

1. **Use only authorized AI tools and platforms officially approved by your department.**
2. **Remove names and sensitive information from prompts and files while using AI tools.**
3. **Review AI-generated content for accuracy and security before using it.**
4. **Promptly report any accidental exposure or upload of confidential data to public AI tools to your IT or Cybersecurity team.**

DON'Ts

1. **Do not input classified government documents, emails, software source code, or citizen PII into public AI tools.**
2. **Do not share admin credentials, API keys, or passwords, with AI tools.**
3. **Do not install unapproved AI extensions or plugins on official devices.**
4. **Do not use AI-generated results without human review.**

RISKS OF NON-COMPLIANCE

- **Exposure of classified national data to external AI training models**
- **Insertion of malicious AI-generated code into government systems**
- **Violation of national cybersecurity policies on data sharing**

Artificial Intelligence (AI) tools enable users to perform tasks more efficiently by generating content, analyzing information, automating routine activities, and supporting decision-making. Their use must be balanced with appropriate security, privacy, and human oversight.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

Secure Use of Removable Media

Guidelines for Secure Use of External Storage Devices

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Ensure secure and authorized use of removable storage media like USB and HDD.

15

ریموواہبل اسٹوریج میڈیا (یو ایس بی، ایچ ڈی ڈی) کا محفوظ اور مجاز استعمال یقینی بنائیں۔

Unsanctioned USB drives and removable media present severe risks of malware insertion, unauthorized data exfiltration, and air-gapped system compromise.

Users must strictly comply with Government of Pakistan's security guidelines when connecting external storage devices to official endpoints.

DO's

1. **Use only officially sanctioned USBs and HDDs approved by your department's IT or Cybersecurity team.**
2. **Scan removable storage devices with updated antivirus software before accessing stored files.**
3. **Maintain physical custody of storage media and lock drives in secure cabinets when not in active use.**
4. **Promptly report lost, stolen, or suspicious storage media to your IT or Cybersecurity team.**

DON'Ts

1. **Do not plug personal USB drives, smartphones, or unvetted media into official devices.**
2. **Do not transfer sensitive, restricted, or classified government data to external media.**
3. **Do not insert unknown USB drives found in public places (USB drop attack risk).**
4. **Do not attempt to bypass USB port block policy, EDR, or other security controls deployed by your department.**

RISKS OF NON-COMPLIANCE

- **Automated malware execution from USBs**
- **Exfiltration of sensitive national data**
- **Violation of data security policies**

Cyber adversaries heavily target **Removable Media & USB Drop Vectors** to breach air-gapped official networks. Always consult your IT or Cybersecurity team before attaching any new physical storage device.

Always protect sensitive files, clear temporary media, and safely hand over unused drives.

16

ہمیشہ اہم فائلوں کو محفوظ کریں، عارضی ڈیٹا مٹائیں اور غیر استعمال شدہ میڈیا واپس کریں۔

Leaving unencrypted files on portable storage or misplacing assigned drives creates severe risks of data theft and leakage.

Every user is individually responsible for safeguarding official files on portable storage, practicing safe cleanup, and returning media to IT team after use.

DO's

1. **Password-protect and encrypt official documents before saving or copying them onto removable drives.**
2. **Safely eject and lock USB drives inside your desk drawer whenever you step away from your workstation.**
3. **Delete temporary official files from portable drives immediately after finishing your tasks.**
4. **Hand over damaged, malfunctioning, or unneeded storage drives directly to your IT team for secure disposal.**

DON'Ts

1. **Do not leave USBs or HDDs unattended on desk tables, in conference rooms, or plugged in overnight.**
2. **Do not place personal photos, private documents, or unvetted media on your assigned official portable drives.**
3. **Do not discard old or broken USB drives in regular office trash cans or recycling bins.**
4. **Do not lend your assigned official storage drives to co-workers, visitors, or family members.**

RISKS OF NON-COMPLIANCE

- **Accidental exposure of confidential government data**
- **Data theft and leakage**
- **Breach of applicable data security and protection regulations**

Deleting a file does not remove its contents from the storage media. Usually, only the reference to the file is removed, while actual data remains on the disk until it is overwritten. Attackers can use data recovery tools to recover deleted files if the storage media is sold or discarded without proper sanitization. **Secure Disposal** methods, such as data wiping, degaussing, or physical destruction, ensure that deleted data cannot be recovered.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

Secure Remote Access

Guidelines for Secure Access to Official Services from Remote Locations

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Access government systems remotely only through approved VPN solutions.

17

سرکاری نظام تک ریموٹ رسائی صرف منظور شدہ وی پی این سے حاصل کریں۔

Exposing official services directly to the Internet invites automated brute-force attacks and persistent cyber attacks from external entities.

Therefore, Government of Pakistan uses secure VPN connections to allow users to securely connect to official services from remote locations.

DO's

1. **Use authorized VPN services provided by your department to remotely connect to official services.**
2. **Set strong authentication credentials on your VPN account.**
3. **Terminate and log out of remote access sessions immediately upon completing official tasks.**
4. **If your VPN connection is unstable or repeatedly disconnects, contact your IT or Cybersecurity team immediately.**

DON'Ts

1. **Do not use unauthorized VPN services or proxy applications for official work.**
2. **Do not disable security controls, such as antivirus, firewall, or endpoint protection, to improve VPN performance.**
3. **Do not leave your VPN session unattended on an unlocked device.**
4. **Do not share your VPN credentials with anyone.**

RISKS OF NON-COMPLIANCE

- **Automated brute-force attacks leading to network perimeter breach**
- **Ransomware deployment across internal server infrastructure**
- **Persistent backdoors allowing covert, long-term espionage**

A **Virtual Private Network (VPN)** is a security technology that creates an encrypted connection between a user's device and an organization's network over the internet. It enables secure remote access to official systems and resources while protecting data from unauthorized access or interception.

Maintain strict meeting privacy and screen confidentiality during remote tele-conferencing.

18

آن لائن اجلاس اور گھر سے کام کے دوران سیکیورٹی اور راز داری کے اصول اپنائیں۔

Unsecured virtual meetings and exposed device screens at home can create high risks of confidential data leaks.

Users should treat their home workspace and online meeting rooms with the same physical and visual privacy standards as official conference rooms and offices.

DO's

1. **Password-protect virtual meetings and enable "Waiting Room" features to vet each attendee prior to entry.**
2. **Use only officially approved tele-conferencing software and tools.**
3. **Position screens away from windows, cameras, family members and house guests while working on official documents.**
4. **Mute microphone and disable webcams when not required, to prevent acoustic or visual leakage during online meetings.**

DON'Ts

1. **Do not post conference meeting links, meeting IDs, or passcodes on public social media or open portals.**
2. **Do not discuss classified or restricted government matters over unencrypted public video conference platforms.**
3. **Do not allow unauthorized household members, guests, or visitors to view or use official equipment.**
4. **Do not record or transcribe sensitive official meetings without prior written authorization from session chairs.**

RISKS OF NON-COMPLIANCE

- **Unauthorized eavesdropping and covert recording**
- **Accidental visual disclosure of sensitive documents**
- **Breach of confidentiality and public disclosure regulations**

A **Meeting Link** is like a digital access key. Anyone who obtains an unauthorized meeting link may attempt to join, listen, access shared content, or disrupt the session. Therefore, meeting organizers must always protect meeting invitations and access credentials.

PKCERT

Ministry of Information Technology & Telecommunication

DIGITAL PAKISTAN

National Cybersecurity Handbook

Incident Response

Guidelines for Recognizing and Reporting Cybersecurity Incidents

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan

Identify cyber security incidents promptly and report them immediately to your local IT or Cybersecurity team.

19

سائبر سیکیورٹی کے واقعات کی فوری نشاندہی کریں اور لوکل آئی ٹی اور سیکیورٹی ٹیم کو رپورٹ کریں۔

Immediate reporting of security incidents prevent localized compromises from escalating into nation-wide disasters.

Delaying incident disclosure impedes containment efforts and significantly increases the risk to government assets.

DO's

1. Learn and understand your department's incident reporting and response procedures.
2. Remain vigilant for unexpected deletion, addition or modification of files, unusual system behavior, and unknown processes.
3. Immediately report any unusual activity that you observe on your devices to your IT or Cybersecurity team.
4. Till the team arrives, isolate machines from local networks (unplug Ethernet cable and turn off Wi-Fi) immediately.

DON'Ts

1. Do not turn off or restart devices showing suspicious activity, as this may erase important data needed for investigation.
2. Do not attempt to self-remediate or run antivirus or data recovery tools on such devices.
3. Do not delay reporting security anomalies out of fear of administrative repercussions or operational disruption.
4. Do not share details or screenshots of active security breaches on public social media or unauthorized chat channels.

RISKS OF NON-COMPLIANCE

- **Rapid lateral malware movement across government network**
- **Irreversible destruction of volatile memory and digital evidence**
- **Extended service downtime and data loss**

Security Incidents include unauthorized access attempts, ransom notes, modified system files, suspicious emails and similar instances causing breach of confidentiality, integrity or availability of information assets. Prompt internal escalation enables local security teams to apply network filters, revoke compromised credentials, and mitigate damage before national infrastructure is compromised.

Provide necessary support during PKCERT-led incident investigations and ensure proper handling of digital evidence.

20

پی کے سرٹ کی زیرِ قیادت تحقیقات میں تعاون کریں اور ڈیجیٹل شواہد کا مناسب تحفظ یقینی بنائیں۔

When critical cybersecurity breaches occur, PKCERT teams conduct in-depth incident investigations and digital forensics to identify root causes, analyze the impact, and contain threats at a national level.

Therefore, users must understand their role and responsibilities in supporting PKCERT to enable an effective and coordinated national incident response.

DO's

1. **Grant immediate, physical and administrative access to affected infrastructure and logs to PKCERT investigation teams.**
2. **Learn basic principles of incident investigation and digital forensics from your IT or Cybersecurity team and PKCERT online resources.**
3. **Preserve digital evidence by maintaining strict chain-of-custody protocols for all impacted devices and storage media.**
4. **Promptly implement emergency containment advisories and remediation guidelines issued by PKCERT investigation teams.**

DON'Ts

1. **Do not alter or overwrite system audit logs, firewall records, or disk memory dumps prior to forensic collection by PKCERT.**
2. **Do not withhold operational details, network diagrams, or incident timelines from PKCERT investigation teams.**
3. **Do not allow unverified third-party vendors or non-cleared staff to tamper with quarantined systems during active inquiry.**
4. **Do not restore operational services or reconnect affected network segments until PKCERT issues formal security clearance.**

RISKS OF NON-COMPLIANCE

- **Incomplete forensic analysis leading to persistent threats**
- **Inability to identify threat actor origin, tactics, and impact**
- **Extended disruption of services**

Under **CERT Rules 2023**, organizations are required to report cybersecurity incidents to PKCERT through approved channels and via organizational, provincial, or sectoral CERTs. Understanding CERT Rules 2023 is a key requirement for ensuring timely and effective incident response, investigation, and mitigation of cyber threats.

Useful Resources

Laws, Rules & Regulations

CERT Rules, 2023
https://pkcert.gov.pk/policies-and-legislation.asp

Electronic Transactions Ordinance (ETO), 2002
https://pkcert.gov.pk/policies-and-legislation.asp

National Cyber Security Policy, 2021
https://pkcert.gov.pk/uploads/2023/06/2021-National-Cyber-Security-Policy-Final.pdf

National Security Policy, 2022
https://pkcert.gov.pk/policies-and-legislation.asp

Pakistan Information Security Framework (PISF), 2026
https://pkcert.gov.pk/grc-policies.asp

Prevention of Electronic Crimes Act (PECA), 2016
https://na.gov.pk/uploads/documents/1470910659_707.pdf

PKCERT

Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

Safeguarding Pakistan's Digital Frontiers

Cybersecurity is everyone's responsibility.

Every secure action strengthens Pakistan's digital future.

info@pkcert.gov.pk | www.pkcert.gov.pk

+92 51 111 162 378

Pakistan's National Cyber Emergency Response Team (PKCERT)
Government of Pakistan