सत्यमेव जयते

Department of Information Technology & Communication, Rajasthan

Cyber Security Best Practices

For

Official Computer Systems Operating on Internal (SecLAN / RajSWAN / RajNET) Networks

*V.**1.0*** *Date: 24-04-2026*

***Contact Us**: Security Operations Center (SOC),*

Department of Information Technology & Communication
Government of Rajasthan

Rajasthan State Data Centre (RSDC-P4), Jaipur

Email: **fms.soc@rajasthan.gov.in**

Table of Contents

Document Control & Contributions

Version	Date	Description of Changes	Prepared By	Reviewed By (L1)	Reviewed By (L2/CISO)	Approved By
0.1	18-02-2026	Initial Draft	Sh. Charu Agarwal	Sh. Pawan Kumar Jangid	—	—
0.2	19-02-2026	Updated after internal review	Sh. Charu Agarwal	Sh. Pawan Kumar Jangid	Sh. Anil Kumar Singh	—
0.3	***27-02-2026***	***Updated after detailed review***	***Sh. Charu Agarwal, ACP(DD) SOC***	***Sh. Pawan Kumar Jangid, AD, OIC(SOC)***	***Sh. Anil Kumar Singh, Director (Technical) & CISO***	***Sh. Himanshu Gupta, COMMISSIONER AND SPECIAL SECRETARY***
1.0	***24-04-2026***	***Final Version***	***Sh. Charu Agarwal, ACP(DD) SOC***	***Sh. Pawan Kumar Jangid, AD, OIC(SOC)***	***Sh. Anil Kumar Singh, Director (Technical) & CISO***	***Smt . Archana Singh, SECRETARY***

SECTION 1: Installation of Antivirus Software on all Internal Systems

(MANDATORY – DO FIRST)

1.1 Install Government-Approved Advanced AV / EDR (Highest Priority)

- Every SecLAN/RajSWAN/RajNET computer must have an approved Antivirus or Endpoint Detection & Response (EDR) solution.
- SecLAN/RajSWAN/RajNET computer systems operate over the official internal Government of Rajasthan networks, which are used for secure communication and data exchange among various government departments and offices across the state including Districts, Blocks and GPs.
- Computers connected to these networks handle sensitive government data, so strict security rules apply.

What you need to do

- download and install it **only from the LAN internal link**:

64-bit systems:

https://172.21.77.106:4343/officescan/download/agent_cloud_x64.msi

32-bit systems:

https://172.21.77.106:4343/officescan/download/agent_cloud_x86.msi

- Follow on-screen instructions and **do not cancel** installation midway.
- Restart your computer if prompted.

Note: If You are not able to complete above steps, then

1.2 Perform Full System Scan Using CSK Bot Removal Tool (NO installation required)

This step ensures that hidden malware or bot infections are removed.

What you need to do

- Open a browser and visit **Cyber Swachhta Kendra (CERT-In initiative):** **https://www.csk.gov.in/security-tools.html**
- Download the **CSK Bot Removal Tool** suitable for your system.

  https://www.k7computing.com/in/k7-bot-removal-tool OR

  https://www.quickheal.co.in/bot-removal-tool

- Run the tool and select **Full System Scan**.
- Allow the scan to complete fully (this may take time).
- If infections are detected, allow the tool to **clean/remove** them.
- Do not use third-party cleaning tools or cracked software.

Imp Note:

1. **Tool mentioned in Point No. 1.2 above is not a substitute for Antivirus / EDR solutions**. All users must continue to maintain the Government-approved Advanced Antivirus / EDR solution (Trend Micro Apex One Agent) on critical office computer systems, as provided through the links mentioned in Section 1.1, to ensure comprehensive protection of Government digital assets.

2. In case a **genuine and fully updated Antivirus (AV) solution** is already installed on your desktop through any authorized channel, apart from as referred to in **Points 1.1 and 1.2 above**, ensure that the solution is **regularly updated** and that **all security modules are enabled** to provide comprehensive protection against multiple types of cyber threats.

3. Further, in the event of receiving any **SOC security alert**, or if the system is suspected to be **compromised or infected**, a **full system scan** must be performed immediately.

1.3 Update Your System Immediately

Unpatched systems are the biggest security risk.

An unpatched system **means that the computer has** known security vulnerabilities that have not been fixed**. Hackers often exploit these weaknesses to:**

- Install malware or ransomware
- Gain unauthorized access to the system
- Steal sensitive information
- Spread infections across a network

- ✓ **Software companies regularly release** security patches and updates **to fix these vulnerabilities.**
- ✓ Installing updates ensures that the system remains protected against newly discovered threats.
- ✓ **For computers running** Microsoft Windows**, these updates are distributed through** Windows Update**, a built-in service provided by Microsoft.**

What you need to do

- Open **Windows Update**.
- Install **all pending updates** (Security updates).
- Restart the system after updates.

Why restarting is necessary

- ✓ **Some updates modify** core system files and security components **that are active while the system is** running. Restarting allows the system to:
- ✓ Apply the updates completely
- ✓ Replace old system files with patched versions
- ✓ Activate new security protections
- ✓ **Without restarting, certain updates may** not take effect**, leaving the system partially vulnerable.**

Benefits of Regular System Updates

Regularly updating the system provides several advantages:

1. Protects against newly discovered cyber vulnerabilities
2. Improves system stability and performance
3. Ensures compatibility with new applications and hardware
4. Strengthens overall cybersecurity of the network

For government or office systems, timely updates are critical because they help **protect sensitive digital assets and prevent cyber incidents**.

Note: Uninstallation of the Trend Micro Apex Agent (deployed on LAN End Points) may be carried out only after obtaining approval from the concerned Department CISO/Dy. CISO or the senior-most DoIT/NIC officer posted there, and only for valid and justified reasons. In such cases, the LAN IP may kindly be shared at **fms.soc@rajasthan.gov.in** and **seclanfms@rajasthan.gov.in** so that the uninstallation process can be undertaken. However, this is advised only in critical circumstances where any legitimate official application is being adversely impacted or prevented from functioning due to the advanced antivirus protection.

SECTION 2: DESKTOP HARDENING & SYSTEM SECURITY (MANDATORY DAILY PRACTICES)

Desktop hardening means securing your computer so that it cannot be misused even if someone tries to attack it. It refers to the process of **strengthening the security of a desktop computer by reducing vulnerabilities and limiting potential attack points**. The goal is to make the system secure so that it **cannot be easily misused, accessed without authorization, or compromised by cyber attackers**.

In simple terms, it means **locking down the computer to prevent misuse or cyber-attacks**.

Objectives of Desktop Hardening

The main objectives are:

- **Protect sensitive data** stored on the computer.
- **Prevent unauthorized access** to the system.
- **Reduce system vulnerabilities** that attackers could exploit.
- **Prevent malware infections** such as viruses or ransomware.
- **Maintain system integrity and reliability.**

2.1 Use Only Genuine and Approved Software

- Ensure your system is running a **genuine operating system**.
- Install **only office-related software**.
- If software is required for official work, **download it only from trusted repository**.
- Never install applications or software from informal, untrusted, or unauthorized sources.
- Do **not install or use**:
    - Cracked or pirated software.
    - Free tools from unknown websites.
    - Torrent, VPN, anonymizer, or screen-sharing tools.

2.2 Work Only as a Normal User

- Do **not** use Administrator account for daily work.
- Administrator access is meant **only for** specific tasks. Ensure administrator credentials are required for installing or modifying software on systems.
- Guest user account must remain **disabled**.

2.3 Keep System Firewall Enabled

A Firewall acts as a security barrier between the computer and external networks such as the internet. It checks data packets entering or leaving the system and blocks suspicious or unauthorized connections.

Most computers running Microsoft Windows include a built-in firewall called Windows Defender Firewall.

- Windows Firewall must **always remain ON**.
- Do not disable firewall for speed, installation, or troubleshooting.
- If any software asks to turn off firewall, do **Cancel**.

2.4. BIOS & Firmware Security

BIOS/UEFI security is an important part of **desktop hardening** because it protects the computer at the **hardware level before the operating system starts**.

- Ensure BIOS/UEFI password is enabled to prevent unauthorized boot access. ***(Remember the password as in case of forgetting the same, you may need to reinstall OS)***

Since BIOS/UEFI controls the boot process, attackers who gain access to it could:

1. Change boot settings
2. Boot the system from external devices (USB/DVD)
3. Bypass operating system security
4. Install malicious software

2.5 Disable Unnecessary System Features

- Remote Desktop (RDP)- **Keep OFF**
- Bluetooth, NFC - **Keep OFF unless officially required**
- Wi-Fi / Hotspot - **Use only approved Wi-Fi network**

Do **not connect office computers** to:

- Personal mobile hotspots
- Smart TVs
- Home IoT devices

2.6 Secure Your Desktop Physically

Physical security of a desktop computer is just as important as digital security. Even if a system has strong passwords, antivirus, and firewall protection, it can still be misused if **someone gains physical access to the computer**. Therefore, users must follow certain practices to prevent unauthorized use.

2.6.1. Lock Your Computer When Leaving Your Desk

Whenever you leave your workstation, even for a short time, you should **lock your computer screen**.

You can quickly lock the system by pressing **Windows + L** on computers running Microsoft Windows.

Locking the computer ensures that:

- No one can access your files or applications.
- Your email or official documents remain protected.
- Unauthorized actions cannot be performed in your name.

When the system is locked, it requires your **login password** to regain access.

2.6.2. Shut Down the System at the End of the Day

At the end of the workday, users should **properly shut down the computer** instead of leaving it running.

Shutting down the system helps to:

- Prevent unauthorized use when the office is closed.
- Reduce the risk of malware or remote attacks.
- Save electricity and improve system performance.

A fresh restart the next day also helps the system **load updates and security configurations properly**.

2.6.3. Do Not Allow Others to Use Your Logged-in System

You should **never allow another person to use your computer while you are logged in**.

Reasons include:

- Actions performed on the system will be **recorded under your user account.**
- Sensitive information may be **accessed or copied.**
- Unauthorized software may be **installed without your knowledge.**

If someone needs to use the computer, **they should log in using their own authorized account**.

SECTION 3: EMAIL SECURITY (MOST COMMON ATTACK VECTOR)

Email is one of the most widely used communication tools in offices and organizations. However, it is also the **most common method used by cyber attackers to launch cyber-attacks**. Because employees frequently receive emails from external sources, attackers often try to exploit this channel to gain unauthorized access to systems and sensitive information.

Cybercriminals use email to deliver various types of threats because it is easy to send malicious messages that appear legitimate. Many attacks rely on **tricking users into clicking harmful links or opening infected attachments.**

Email security is critical because email is the most common entry point for cyber-attacks. Attackers use phishing, malicious links, and infected attachments to compromise systems. Following proper email security practices helps protect both individual systems and the organization's digital infrastructure.

Common threats delivered through email include:

- Phishing emails **that try to steal passwords or confidential information.**
- Malware attachments **that infect the system when opened.**
- Ransomware links **that download malicious software.**
- Fake messages impersonating **officials or trusted organizations.**

Importance of Email Security:

Strong email security practices help to:

- **Protect** sensitive organizational data.
- **Prevent** malware infections.
- **Avoid** unauthorized system access.
- **Reduce the risk of** financial or data loss.

3.1 Use Only Official Government Email

- Use only your official email ID (ending with **rajasthan.gov.in/rajpolice.gov.in…etc**).
- Never forward official documents to:
    - Personal cloud accounts.

Do **not register official email IDs** on:

- Social media
- E-commerce portals
- Third-party tools or websites

3.2 Identify Phishing Emails

Be alert if an email:

- Asks for passwords, OTPs, or money
- Creates urgency ("Account will be blocked")
- **Has spelling mistakes** or unusual sender address
- Contains unknown attachments or shortened links

IMP: Do not click. Do not reply. Report immediately to fms.soc@rajasthan.gov.in

---

3.3.URL & Domain Verification:

Inculcate the habit of verifying domain names, URLs & email attachments carefully before clicking, especially in emails and messages. (May refer publicly available Threat Intel resources like virus total etc.)

URL & Domain Verification means carefully checking the **website address (URL), domain name, or links in emails/messages** before clicking them. Many cyber-attacks such as **phishing, malware delivery, and credential theft** rely on tricking users into clicking fake or malicious links. Developing the habit of verifying these elements can prevent many security incidents.

1. Check the Domain Name Carefully
2. Hover Over Links Before Clicking
3. Verify the Full URL Structure
4. Use Threat Intelligence Tools
5. Be Cautious with Email Attachments
6. Look for HTTPS but Don't Fully Trust It

3.4 Safe Email Practices

Safe Email Practices help reduce the risk of **phishing attacks, account compromise, and malware infections**. Following a few disciplined practices when using email can significantly improve personal and organizational cybersecurity.

3.4.1. Disable "Save Password" in Browser

Many browsers offer the option to save email login passwords automatically. While convenient, this can be risky.

Why it is risky:

- Anyone with access to your device can open your email account.
- Malware or browser vulnerabilities may extract saved credentials.

- Shared or office computers **increase** the risk of unauthorized access.

Best practice:

- Avoid storing email passwords in the browser.
- Use a trusted password manager.
- Always enable **multi-factor authentication (MFA)** for email accounts.

3.4.2. Do Not Auto-Download Attachments

Some email applications automatically download attachments when an email is opened. This can expose the system to malware or malicious scripts**.**

Risks of auto-downloading attachments:

- Malware hidden inside documents or archives can be downloaded automatically.
- Attackers often disguise malicious files as invoices, reports, or delivery notices.
- Some files can exploit vulnerabilities immediately upon download.

Best practice:

- Disable automatic attachment downloads in your email settings.
- Only download attachments from trusted and verified senders.
- Scan suspicious files using tools.

3.4.3. Forward Emails Only When Necessary and Keep the Full Trail

Forwarding emails unnecessarily can expose sensitive information, internal discussions, and contact details.

Risks of careless forwarding:

- Confidential information may reach unintended recipients**.**
- Attackers can gather information from email chains for social engineering attacks.
- Removing parts of the email trail may cause miscommunication or loss of context.

Best practice:

- Forward emails **only when required for work or communication**.
- Keep the **complete email thread (trail)** so recipients understand the context.
- Remove sensitive information if it is not relevant to the recipient.

SECTION 4: INTERNET & BROWSER SECURITY

Web browsers store a lot of information such as login sessions, cookies, and browsing data. If these settings are not configured securely, attackers may exploit them to **steal credentials, track user activity, or gain unauthorized access to accounts**. Configuring secure browser settings helps protect personal and organizational data.

4.1 Use Secure Browser Settings

Ensure:

- Enhanced Security Mode is enabled.
- Most modern browsers provide a **built-in enhanced security or protection mode** that improves protection against malicious websites and downloads.
- On browser exit, it automatically clears:
    - Cookies
    - Cache
    - Browsing history
    - Stored passwords

Benefits of enabling enhanced security mode:

- Detects and blocks phishing websites
- Warns users before visiting dangerous or suspicious sites
- Provides stronger protection against malicious downloads
- Uses real-time security checks to identify harmful URLs

4.2 Internet Usage Rules

Following responsible internet usage practices is important to maintain **organizational security, productivity, and protection against cyber threats**.

Many websites that provide pirated content or free downloads are commonly used by attackers to distribute **malware, spyware, and phishing links**.

Employees should therefore restrict browsing to **work-related and trusted websites only**.

Do not visit:

- **Torrent sites**- Torrent websites allow users to download files through peer-to-peer sharing. While some torrents may contain legitimate content, many are used to distribute **pirated software, movies, or games**.
- **Streaming sites**- Unverified streaming websites that offer **free movies, TV shows, or sports broadcasts** often operate illegally and may host harmful content.
- **Free movie / software & crack sites**- Websites that provide **free premium software, cracks, or pirated applications** are a common source of cyber threats.

Use only **work-related websites**.

4.3 Avoid Public Wi-Fi

Public Wi-Fi networks are often **unsecured or poorly protected**, which makes them an easy target for cyber attackers. When users connect to such networks, sensitive data such as **login credentials, official documents, or session information** may be intercepted. Therefore, government systems and important official portals should **never be accessed from public or open Wi-Fi networks**.

Never access government systems & imp government portals from:

- **Railway Wi-Fi**- Free Wi-Fi services available at railway stations are open networks used by a large number of people.
- **Cafe Wi-Fi**- Public Wi-Fi available in cafés or restaurants is generally **shared by many unknown users** and often has limited security controls.
- **Airport public networks**- Airports commonly provide free internet access for passengers, but these networks are **frequently targeted by cybercriminals** because of the large number of users.

4.4 social media & Messaging Platforms

- Do not use official email IDs for registration on social media or non-official platforms.
- Do not share official information, photographs, screenshots, or documents on social media.
- Avoid clicking links or downloading files received through messaging platforms.
- Enable privacy settings at the highest level and avoid public visibility.

4.5. Secure Browser Usage for Sensitive Access

•When accessing **government applications, official email services, or other sensitive online portals**, it is important to use secure browsing practices. One recommended method is to use the **Private or Incognito browsing mode** available in most modern browsers.

For example, browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge provide a **Private/Incognito mode** that helps reduce the amount of browsing data stored on the device.

Private or Incognito mode is a browser feature that allows users to browse the internet without saving browsing activity on the local device. Once the browsing session is closed, most of the temporary data generated during that session is automatically deleted.

4.6. Browser Extensions & Toolbar Control

Browser extensions, toolbars, and add-ons can enhance browser functionality, but they can also introduce **serious security risks** if installed from untrusted sources.

Many malicious extensions are designed to **collect user data, monitor browsing activity, inject advertisements, or steal login credentials**.

Therefore, users should **not install third-party browser toolbars, download managers, or add-ons unless they are explicitly approved by the organization's IT or security team**.

4.6.1. Risks of Unapproved Browser Extensions

Unverified browser extensions may contain hidden malicious code.

4.6.2. Risks of Browser Toolbars

Third-party browser toolbars often request **extensive permissions** within the browser.

4.6.3. Risks of Download Managers and Add-ons

Many download managers and add-ons available online are bundled with **adware or spyware**.

SECTION 5: PASSWORD & ACCESS MANAGEMENT

5.1 Create Strong Passwords

Passwords are the **first line of defense** for protecting user accounts, government systems, and sensitive data. Weak or predictable passwords make it easier for attackers to gain unauthorized access through methods such as **brute-force attacks, password guessing, or credential stuffing**. Therefore, users must always create **strong and secure passwords**.

Your password must:

- Be at least **8 characters**
- Include:
    - Capital letters
    - Small letters
    - Numbers
    - Special characters

Do not use:

- Name, DOB, mobile number
- Same password for multiple systems
- Regularly change passwords for network systems and applications and strictly avoid reusing passwords across multiple accounts.
- Using the same password across multiple websites or systems increases risk. If one account becomes compromised, attackers may attempt to use the same password to access **other services or official portals**.
- Each important account should have a **unique password**.

5.2 Enable Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) adds an extra layer of security to user accounts by requiring **more than one method of verification** before granting access.

Even if a password is compromised, MFA helps prevent unauthorized users from accessing the account.

Therefore, MFA should always be enabled wherever it is available, especially for **government systems, official email accounts, and sensitive portals**.

- Always enable MFA where available.
- Never share OTPs with anyone.
- Many platforms support MFA, including services like Google Authenticator and Microsoft Authenticator, which generate secure one-time verification codes.
- Cybercriminals often attempt to trick users into revealing OTPs through **phishing emails, fake calls, or fraudulent messages**.
- Attackers may pretend to be **technical support staff, bank officials, or system administrators** and request OTPs for verification.

5.3. Password Handling Discipline

Maintaining proper discipline in handling passwords and other sensitive information is essential for protecting **organizational systems, networks, and confidential data**. Writing passwords or system details in visible places can expose them to unauthorized individuals and significantly increase the risk of **security breaches or unauthorized access**.

• Do not write passwords, IP addresses, or sensitive information on paper, sticky notes, or visible surfaces.

• Use Secure Methods for Storing Credentials.

• Maintain Clean Desk Practices.

SECTION 6: USB, FILES & DATA HANDLING

6.1 External Devices

External storage devices such as USB drives, external hard disks, and other removable media can be convenient for transferring data, but they also pose **significant cybersecurity risks**. These devices may carry **malware, viruses, or unauthorized software** that can compromise office systems and networks. Therefore, strict precautions must be followed when handling external storage devices in the workplace.

- Personal USBs and hard disks are **not to be used at work place.**
- Use external devices only after proper sanitization.
- Disable **autoruns** for removable media.
- Never use promotional or unknown USB devices.
- Never directly insert any **USB** storage device in office computers as the unknown USB's may contain malware. First Scan such storage before opening and using the files inside.

6.2 File Protection

- **Password-protect sensitive files and keep them in compressed format:**
  Important or confidential files should be protected with strong passwords to prevent unauthorized access. Compressing files using tools like ZIP or RAR with password protection adds an extra layer of security and makes files easier to store or share securely.
- **Store official data only on Office PCs:**
  All official documents and work-related data should be saved only on authorized office computers or approved systems. This helps maintain data security, ensures proper backup, and prevents the risk of data loss or leakage that could occur if files are stored on personal devices.

6.3. Printer & Peripheral Security

6.3.1 Ensure printer firmware and software are regularly updated:

Printers and other peripherals often receive firmware and software updates from manufacturers to fix security vulnerabilities and improve performance. Regularly installing these updates helps protect the device from potential cyber threats and ensures it operates safely within the organization's network.

6.3.2 Configure unique PIN/password for shared printers:

Shared printers should be secured with a unique PIN or password to prevent unauthorized users from accessing them. This helps ensure that only authorized employees can print, modify settings, or retrieve sensitive documents from the printer.

6.3.3 Disable direct internet access on printers:

Printers should not have unrestricted access to the internet. Disabling direct internet connectivity reduces the risk of external attacks, malware, or unauthorized remote access. Printers should only communicate through the secure office network.

6.3.4 Configure printers to avoid storage of print history or documents:

Some printers store copies of printed documents or maintain a print history in their internal memory. These settings should be disabled or cleared regularly to prevent sensitive information from being stored and potentially accessed by unauthorized users.

SECTION 7: POST-REMEDIATION MONITORING

7.1 Observe System Behavior (Next 24–48 Hours)

After resolving a potential issue or security incident, the system should be carefully monitored for the next 24–48 hours to ensure that no hidden threats or problems remain. Pay attention to the following warning signs:

- **Unusual slowness:**

  If the computer suddenly becomes slower than normal, takes longer to open applications, or frequently freezes, it may indicate that a malicious program or background process is consuming system resources.

- **Automatic pop-ups:**

  Unexpected pop-ups, advertisements, or browser windows opening on their own can be a sign of adware, malware, or unauthorized software installed on the system.

- **Unknown processes:**

  Check the system's task manager for unfamiliar or suspicious processes running in the background. Unknown programs consuming high CPU, memory, or disk usage may indicate malicious activity.

- **Repeated antivirus alerts:**

  Frequent antivirus warnings or detections could mean that a threat still exists on the system or that new suspicious files are being created.

Action if any issue is noticed:
If any of the above signs appear, immediately take a complete backup of important data and consider rebuilding the PC (reinstalling the operating system and required software) to ensure the system is fully clean and secure. This helps eliminate any hidden malware that may not have been removed earlier.

7.2 Reporting & Closure

After completing the system checks and remediation steps, proper documentation and reporting should be done to formally close the incident or security review. The following information should be shared:

- **Antivirus / EDR scan report:**

  Provide the latest scan report generated by the installed Antivirus or Endpoint Detection and Response (EDR) solution. The report should clearly show whether any threats were detected, quarantined, or removed from the system. This helps the security team verify that the system has been properly scanned and is safe to operate.

- **CSK scan result：**

  If a CSK security scan or any internal security scanning tool was used, share the complete scan results． These results help confirm that the system does not contain vulnerabilities, malicious files, or suspicious configurations．

- **Submit details to SecLAN/RSWAN/SOC Team for formal closure：**

  All reports and relevant details should be submitted to the SecLAN, RSWAN, or SOC（Security Operations Center） team for review． The security team will analyze the reports provided and confirm that the issue has been resolved． Once verified, they will formally close the case or incident in the security monitoring system．

Proper reporting ensures accountability, documentation, and compliance with organizational security policies.

SECTION 8: IMPORTANT SUPPORT & REFERENCES

SN	Resource URL	Description
1	https://doitc.rajasthan.gov.in/Content/CyberSecurityAdvisory.aspx	DOITC Cyber Advisories
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://www.csk.gov.in	Security Tools & Best Practices
4	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
5	https://infosecawareness.in/	Security Awareness materials
6	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
7	https://guidelines.india.gov.in/	Guidelines for Indian Government Websites