

**SHAHEED HIMAYUN MUZZAMIL MEMORIAL**

**Govt. Degree College, Anantnag**

Khanabal, Anantnag - 192101 (J&K) NAAC ACCREDITED GRADE "B+" (CGPA: 2.53)

No DCA/Nodal/24/2394

Dated :- 14-12-2024

The Principal  
Govt. Degree College,  
Anantnag (Women) /Bijbehara/ Dooru/  
Uttersoo/ Verinag / Mattan / Kokernag/ Larnoo/Qazigund.

**Subject: - Cyber security compliance checklist for all Departments- District Anantnag.**

Sir/Madam,

Kindly find enclosed herewith the Cyber security compliance checklist issued by Deputy Commissioner Anantnag for favour of further necessary action at your end please.

Thanking you,

Yours Sincerely,

  
{Prof. Muzafar Ahmad Bhat}

Principal

Copy to :-

1. Office records.

Participate Boys Dept  
to be forwarded to all GDC's of District Anantnag



GOVT OF JAMMU AND KASHMIR  
DEPUTY COMMISSIONER/DISTRICT MAGISTRATE ANANTNAG.  
Email: [anantnag@nic.in](mailto:anantnag@nic.in) Phone No. : 01932-222337

**Subject: - Cyber Security Compliance Checklist for all Departments-District Anantnag.**

With the ubiquitous applications of Information and Communication Technologies (ICT) in almost all facets of service delivery and operations, continuously evolving cyber threats have become a concerned for the Government. Cyber-attacks can come in the form of malware, ransom ware, phishing, data breach etc. that adversely affect an organization's information and systems. Cyber threats leading to cyber-attacks or incidents can compromise the confidentiality, integrity and availability of an organization's information and systems and can have far reaching impact on essential services and national interests.

The ICT infrastructure of the government entities is one of the preferred targets of the malicious actors. The responsibility of implementing good cyber security practices for protecting computers, servers, applications, electronic systems, networks and data from digital attacks, also remain with the government entity.

Keeping the above facts into consideration, it is requested to all stake holders to adhere the following security tips:

**A) Browser Security Tips :**

1. Always update your web browser with the latest patches.
2. Disable pop-up windows in your browser.
3. Delete browser cookies and cache regularly.
4. Enable private browsing or incognito mode.
5. Be careful with the websites/links you visit.
6. Use privacy or security settings that are inbuilt into the browser.
7. Disable the login and password remember option.
8. Enable warn the user option when websites try to install extensions or themes.
9. Enable "Safe search" ON in search Engines.

1. Install software like pop-up ad blocker to block the malicious advertisements appearing on websites.
2. Always keep your browser updated.
3. Install antivirus and antimalware solutions in your devices and keep them updated.
4. Check the links before clicking.
5. Hover over the images/links to find the actual link.

#### **(F) Identity Theft Scams :**

Fraudsters take advantage of user's carelessness and lack of know-how of the privacy settings, which allow them to commit fraud by accessing another person's personal information- like their name, identifying number, or credit card number, without their permission.

#### **(G) Loan APP Scam**

There are many unregistered digital lending apps, which provide instant loans. These apps may get access to your personal information and data stored in your mobile. Mostly, the operators are not registered with the RBI as lenders and are therefore illegal. These apps charge higher rate of interest and penalties.

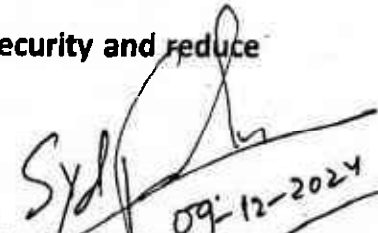
##### **Safety tips**

- I. The borrower should have checked if the lender is approved by RBI and is associated with a financial institution.
- II. Always check the terms and conditions of lending, genuineness of their website, physical office locations, Company Identification Number (CIN), and details of the Certificate of Registration (CoR).
- III. Do not share your personal details with anyone on social media.
- IV. Bank officials, financial institutions, RBI, and/or any genuine entity never ask customers to share confidential information such as username, password, card details, CVV, or OTP.
- V. Always check URL and domain names received in emails for spelling errors. Visit only the official website of your bank or service provider.
- VI. Do not enter your PIN or password anywhere to receive money.
- VII. Do not download an application from any unknown sources.
- VIII. Check the permission(s) and access it seeks, such as contacts, gallery etc.
- IX. Only give access to those permissions which are absolutely required by the application.

**) Additional Precautions :**

1. Update your operating system, browsers, plugins, and software to the latest version.
2. Remove unauthorized software (especially legacy programs).
3. Enable the firewall and install suitable anti-malware, anti-ransomware, and anti-exploit software.
4. Configure regular system scans.
5. Disable unnecessary network ports and services.
6. Please report any cyber related fraud/threats to Cyber Crime branch of Police and also alert your officers/sub-ordinates.
7. Any cyber related threats and security breaches may also be reported to **Indian Computer Emergency Response Team (CERT-in)**

**By following these guidelines, you can enhance your security and reduce the risks of online threats.**

  
09-12-2024  
Deputy Commissioner  
Anantnag  
Dated: - 09-12-2024

**No: DCA/Ang/2024/90055-87**

Copy to the: -

1. Divisional Commissioner, Kashmir.
2. All Sectoral/District Heads for information and compliance.
3. Office file.