MINISTRY OF DEFENCE
CYBER CELL

CYBER SECURITY ADVISORY 01/2020
CYBER SECURITY BEST PRACTICES FOR PROTECTION OF PII RELATED TO SERVICE PERSONNEL

1. **Personally Identifiable Information (PII)**. PII is any data that could potentially be used to identify a particular person. Example include full name, Mobile Number, Office/ Residence Address, Aadhaar Number, PAN Number, Driver's license Number, Bank Account Number, Passport Number of self and family member, etc.

2. **Misuse of PII by Malicious Actors**. Malicious actors can misuse PII by stitching together, various disparate information, to their own advantage for carrying out targeted spear-phishing attack. For example, if an e-mail of Service Personnel is compromised, the same can be used for malicious activities like breach of privacy, phishing, illegal activities, blackmailing the victim for money or leakage of official secrets. Identity theft of one's Credit/ Debit card info can result in loss of money by fraudulent transactions on behalf of the victim. In case of loss of Aadhaar, PAN, Driving License etc, the same can be used to avail fake loans or can be used as an ID proof while committing a crime. These ID proof can be used to purchase SIM cards for criminal purpose. Using Departmental ID cards, one can enter in restricted or prohibited area for any anti-national activities. Death benefits of an individual like insurance can be claimed by frauds by using fake ID cards of the heirs. Medical and children identity can be used to avail benefits of medical insurance claim and education grants/loans.

3. PII is stored in digital format at various locations/ devices in the organisations, such as web application servers, email servers, end point devices and can be compromised by carrying out targeted attack on them. The same can be carried out through the usage of external media such as Wireless/ USB devices used for storage & transfer of data. **The best practices in the succeeding paragraphs will aid an organisation/ individual user in maintaining good Cyber Security Hygiene and thus protect the PII.**

4. **Web Applications Security Best Practices.** Internet facing websites of organisations are always subjected to regular online attacks by adversaries/ hackers. These websites may contain sensitive PII of service personnel. Therefore, these websites are to be protected with adequate security controls. Some of the best practices in this regard are enumerated below:-

(a) **Use https protocol instead of http protocol** as it has inherent security and prevents Man-In-The-Middle (MITM) attack.

(b) **Carry out Vulnerability Assessment/ Security Audit** of Internet facing websites regularly from **CERT-In empaneled vendors.**

(c) For **security of data at rest (database) and data in use,** an **appropriate encryption algorithm must be used along with layers of security.**

(d) Security of PII data on Internet facing website should be taken care using necessary security controls/ techniques like encryption, anonymization and tokenization etc.

(e) In case site uses SSL, the **SSL certificate should be signed by an authorised CA/ RA approving authority.** The same needs to be kept current.

(f) **Download any software from original websites,** rather than third party.

(g) **Install & configure software firewall** to protect against malicious traffic.

(h) **Use Certified / PCI Compliant payment gateway** for online transactions.

5. **Email Security Best Practices.** Email needs to be kept secure and free from the malicious content to keep the potentially sensitive information from being read by an unintended user. Following actions are recommended:-

(a) Use strong passwords for email account.

(b) Scan the emails with latest update Spyware and antivirus prior to opening it.

(c) Do not open email attachments from unknown sources.

(d) Do not click on the embedded links in emails.

(e) Empty the spam & trash folder regularly.

(f) Encrypt/ Password protect the documents used in emails for exchange of important information.

6. **Desktop Security Best Practices.** The following are the best practices to be followed for protection of desktop clients:-

(a) Always use licensed software so that you have regular updates of your OS and applications.

(b) Read terms & Conditions/ Licensed agreement provided by vendor/software before installation.

(c) Properly shutdown the PC. Never switch off directly from main supply.

(d) Enable auto updates of OS/ AV so as to update regularly.

(e) Install antivirus/ antispyware & update it regularly.

(f) Secure data at rest with encryption. Dispose sensitive data securely using digital file shredder software.

(g) Use strong & long password for login in to client and applications too.

(h) Periodically backup the data for computer on other media.

(j) Enable BIOS password to prevent unauthorized access to PC.

(k) Enable screen lockout option.

(l) Beware of personnel around the office, against shoulder surfing.

(m) Do not store unauthorized/ service related data on PCs.

7. **Wireless Security Best Practices**. Technology has made life convenient for everyone to connect to the Internet without having to connect physically to the networking devices through technologies such as Wi-Fi and Bluetooth. Both Wi-Fi and Bluetooth rely

on radio signals for transmission of data. Radio signals are relatively easy to intrude upon when compared to tapping information on a cable making them more susceptible to an attack. The following are the few of the best practices to be followed for a safe wireless networking experience:-

(a) Change default admin password.

(b) Use WPA3 security, along with strong encryption algorithm (AES-256)

(c) Change default SSID and do not enable SSID broadcast.

(d) Enable MAC filtering.

(e) Turn off the Wi-Fi when not in use.

(f) Assign static IP address to devices and turn OFF DHCP.

(g) Do not enable auto connect to open Wi-Fi network.

8. **USB Security Best Practices**. Use of portable devices can increase the risk of data loss, data exposure and increased exposure to network based attacks to and from any system the device is connected to. The following are some of the best practices to be followed for USB security:

(a) Scan the portable device with latest updated antivirus before its usage.

(b) Protect USB with password, in case the facility is provided on it.

(c) Encrypt files & folders on USB.

(d) Protect the stored documents with strong password.

(e) Do not accept any promotional USB device from unknown persons.

(f) Never keep sensitive information on USB without encryption.

(g) Safely and securely destroy/dispose the old media with stored data.

(h) Strictly control the use of USB/removable media for storing/processing/ transfer of official/ sensitive data.

9. **Best Practices for Protection from Phishing.** Phishing is when cybercriminals send malicious emails designed to trick people into falling for a scam. The intent is often to get users to reveal financial information, system credentials, or other sensitive data. The following best practices may be followed for the protection from phishing:-

(a) Never click on unknown links.

(b) Do not open unknown attachments and mails received from unknowns sources.

(c) Always check for misspelled URL against the genuine ones.

(d) Check for padlock & secure channel for banking and transactions (https & Padlock).

(e) Never reply to emails that ask for your personal information like Service information or PII. Always view any email request for financial or other personal information with suspicion, particularly and **'*urgent*'** request. When in doubt do not respond to questionable email or enter information on questionable websites. Check on phone to verify from the originator.

10. **Web Browser Security Best Practices.** Web browsers are designed to store information for user's convenience but that information can fall into wrong hands. Unless properly configured, most browsers contain vast amounts of private information that is forwarded to the company which owns the browser. The information can also be potentially exploited or collected by third parties by various means including by enticing people to add various plugins. ***Awareness of security threats, choice of right web browser as well as security configurations can make a huge difference to personal safety and security while browsing.*** Following guidelines should be adhered to while using web browsers and search engines to avoid any loss of data/ privacy/ money and avoid targeted cyber-attack through phishing etc.:-

(a) Choose a secure browser that protects your privacy. This is absolutely essential for staying safe online and keeping data secure from third parties.

(b) Update your browser time to time or enable auto update to prevent attacker from exploiting emerging vulnerabilities.

(c) Configure privacy and Security settings of the browser to avoid being monitored and for enhanced security. For example, clear web browser cache, use incognito mode etc.

(d) Run Anti-Virus Software and Scan Files before Downloading.

(e) Use HTTPS mode for browsing. The 's' in "https" stands for secure, meaning that the website is employing SSL encryption. Check for an "https:" or a padlock icon in your browser's URL bar to verify that a site is secure before entering any personal information.

(f) Don't reuse the passwords. Using the same password for multiple sites only makes it easier for attackers to compromise your sensitive information. It is also recommended to frequently change the passwords.

(g) Do not save credentials in the browser.

(h) Disable *Auto-Complete for Forms / Remember Passwords* Features.

(j) Popup blocking is now a standard browser feature and should be enabled while surfing the web.

(k) Don't visit the malicious websites. Even if you have high security settings and anti-virus software, visiting malicious a websites can result in downloading of viruses, spyware or ransomware.

11. **Best Security Practices for Individuals.** The following best practices may be followed by Individuals:-

(a) Do not keep Personnel Identifiable Information (PII) on Internet systems.

(b) Do not share your mobile number and email ID with unauthorised agencies.

(c) Take precaution while using social medial platforms. Avoid unknown people on social media for any interactions. Be aware of shoulder surfing personnel.

(d) It should be ensured that there is no unauthorized possession/ processing of sensitive information in digital form by service personnel on their devices.

(e) Personal identity by way of designation, appointment, official address or posting photograph in office premises on social networking sites for government personnel/ member representative of establishment / organisations must not be made public.

(f) Personnel must not create or join communities/groups/email IDs revealing course, batch, establishment/office or any affiliation with defence.

(g) Personnel of establishment/ organizations must avoid uploading PII/ sensitive data/ documents to cloud services.