भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

**Draft Master Directions for Comments**

CO.DPSS.OVRST.No.xx / xxxx / 2023-24 June 02, 2023

The Chairman / Managing Director / Chief Executive Officer
Authorised Non-bank Payment System Operators

Madam / Dear Sir,

**Draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators**

Ensuring safety and security of payment systems is a key objective of the Reserve Bank. To ensure that the authorised non-bank Payment System Operators (PSOs) are resilient to traditional and emerging information systems and cyber security risks, it is proposed to issue Directions, covering robust governance mechanisms for identification, assessment, monitoring and management of these risks. The Directions shall also cover baseline security measures for ensuring system resiliency as well as safe and secure digital payment transactions. However, they shall endeavour to migrate to latest security standards. The existing instructions on security and risk mitigation measures for payments done using cards, Prepaid Payment Instruments (PPIs) and mobile banking continue to be applicable as hitherto.

2. These Directions are issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

Yours faithfully,

(P Vasudevan)
Chief General Manager-in-Charge

भुगतान और निपटान प्रणाली विभाग, केंद्रीय कार्यालय, 14 वी मंजिल, केंद्रीय कार्यालय भवन,शहीद भगत सिंह मार्ग, फोर्ट, मुम्बई - 400001
फोनTel: (91-22) 2260 1000; फैक्सFax: (91-22) 2265 9566; ईमेल-e-mail : cgmdpssco@rbi.org.in
Department of Payment and Settlement Systems, Central Office, 14th Floor, Central Office Building, Shahid Bhagat Singh Road, Fort, Mumbai -400001

# Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators (PSOs)

## Section I

## Preliminary

### Introduction

**1.** In exercise of the powers conferred under Section 10 (2) read with Section 18 of the Payment and Settlement Systems Act, 2007 (PSS Act), the Reserve Bank of India (RBI, Bank) being satisfied that it is necessary and expedient in the public interest so to do, issues the Master Directions hereinafter specified.

### Short Title and Commencement

**2.** These Master Directions shall be called the Reserve Bank of India (Cyber Resilience and Digital Payment Security Controls for PSOs) Master Directions, 2022 (Master Directions, Directions).

**3.** The Directions shall come into effect on the day they are placed on the official website of the RBI. In order to provide adequate time to put in place the necessary compliance structure, a phased implementation approach[1] is prescribed as under –

| Regulated Entity | Timeline |
|---|---|
| Large non-bank PSOs[2] | April 1, 2024 |
| Medium non-bank PSOs[3] | April 1, 2026 |
| Small non-bank PSOs[4] | April 1, 2028 |

### Applicability

**4.** The provisions of these Directions shall apply to all authorised non-bank PSOs.

---

[1] The timelines prescribed in the instructions issued earlier by RBI shall continue to be applicable as hitherto.

[2] For the purpose of these Directions, Clearing Corporation of India Limited (CCIL), National Payments Corporation of India (NPCI), NPCI Bharat Bill Pay Limited, Card Payment Networks, Non-bank ATM Networks, White Label ATM Operators (WLAOs), Large PPI Issuers, Trade Receivables Discounting System (TReDS) Operators, Bharat Bill Payment Operating Units (BBPOUs) and Payment Aggregators (PAs) are considered as large non-bank PSOs.

[3] Cross-border (in-bound) Money Transfer Operators under Money Transfer Service Scheme (MTSS) and Medium PPI Issuers are considered as medium non-bank PSOs.

[4] Small PPI Issuers and Instant Money Transfer Operators are considered as small non-bank PSOs.

Categorisation of authorised non-bank PPI Issuers into small, medium and large is as per the Oversight Framework for Financial Market Infrastructures (FMIs) and Retail Payment Systems (RPSs). If a PPI Issuer moves to a higher category, the timeline of the category to which it moves into, would apply. For instance, if a small (or medium) PPI issuer moves into medium category (or large), it will need to comply with these Directions within a period of two years from the time of new categorisation.

**5.** To effectively identify, monitor, control and manage cyber and technology related risks arising out of linkages of PSOs with unregulated entities who are part of their digital payments ecosystem (like payment gateways, third party service providers, vendors, merchants, etc.), PSOs shall ensure adherence to these Directions by such unregulated entities as well, subject to mutual agreement. An organisational policy in this respect, approved by the Board, shall be put in place.

**Purpose**

**6.** These Directions aim to improve safety and security of the payment systems operated by PSOs by providing a framework for overall information security preparedness with an emphasis on cyber resilience.

## Section II
## Governance Controls

**7.** The Board of Directors (Board) of the PSO shall be responsible for ensuring adequate oversight over information security risks, including cyber risk and cyber resilience. However, primary oversight may be delegated to a sub-committee of the Board which shall meet at least once every quarter.

**8.** The PSO shall formulate a Board approved Information Security (IS) policy to manage potential information security risks covering all applications and products concerning payment systems as well as management of risks that have materialised. The policy shall be reviewed annually. It shall cover at the minimum, (i) roles and responsibilities of Board / sub-committees of the Board, senior management and other key personnel; (ii) measures to identify, assess, manage and monitor cyber security risk which shall also include various types of security controls for ensuring cyber resiliency along with processes for training and awareness of employees / stakeholders.

**Cyber Security Preparedness**

**9.** The PSO shall prepare a distinct Board approved Cyber Crisis Management Plan (CCMP) to detect, contain, respond and recover from cyber threats and cyber attacks. Relevant guidelines from CERT-In / National Critical Information Infrastructure Protection Centre (NCIIPC) / IDRBT and other agencies may be referred for guidance.

**Risk Assessment and Monitoring**

**10.** The Board shall entrust the responsibility and accountability for implementing the IS policy and the cyber resilience framework as well as for continuously assessing the overall IS

posture of PSO to a senior level executive. [e.g. Chief Information Security Officer (CISO)].

**11.** The PSO shall define appropriate Key Risk Indicators (KRIs) to identify potential risk events and Key Performance Indicators (KPIs) to assess the effectiveness of security controls. These KRIs and KPIs shall be continuously monitored by the sub-committee of the Board referred to in paragraph 7.

**12.** The PSO shall, undertake a cyber risk assessment exercise relating to launch of new product / services / technologies or undertaking major changes to infrastructure or processes of existing product / services. Action points emanating from such assessment shall be implemented under the oversight of the CISO or equivalent executive.

## Section III

## Baseline Information Security Measures / Controls

**13. Inventory Management**

(a) The PSO shall maintain a record of all the key roles, information assets (applications, data, infrastructure, personnel, services, etc.), critical functions, processes, third-party service providers and their inter-connections and classify and document their levels of usage, criticality and business value.

(b) A complete process flow diagram of network resources, inter-connections and dependencies, and data flows with other information assets, including any other third-party systems, shall be created and maintained.

(c) Asset information shall necessarily include an identifier, network address, asset location, asset owner name and End of Life Support (EoLS). All assets (hardware or software) approaching EoLS shall be assessed to evaluate risks associated with the continued use of the unsupported asset.

**14. Identity and Access Management**

(a) Policies, procedures and controls that address access privileges as well as administration of access rights must be established.

(b) All individuals having access to the IT environment of the PSO shall be assigned a digital identity, which shall be maintained and monitored till termination.

(c) Default authentication settings in systems / software / services shall be deactivated and changed before they are put to live environment.

(d) Access to systems and different environments (development, test, production, etc.) shall be based on need-to-have, need-to-know and based on the principle of least privilege[5].

(e) The use of privileged accounts[6] shall be with multi-factor authentication and tightly monitored. Appropriate controls, including rotation policy, shall be implemented.

(f) Necessary security controls, including centralised mechanism to whitelist / blacklist, shall be put in place to ensure secure use of removable media and portable devices (eg. smartphones, laptops, etc.).

(g) In case of remote / work from home situations, adequate precautions, including multi-factor authentication mechanism, shall be in place.

(h) The PSO shall define and implement procedures that limit, lock and terminate system and remote sessions after a pre-defined period of inactivity.

(i) PSO shall have physical and environmental safeguards, with periodic testing, to protect access to its information assets from natural disasters and other threats.

**15. Network Security**

The PSO shall put in place the following measures to protect its network and systems from external threats:

(a) Network devices shall be configured and checked periodically for security rules;

(b) A Security Operations Centre (SOC) shall ensure proactive and centralised monitoring of comprehensive network and system logs collected and management of security incidents with effective tools for detection, escalation and quick response;

(c) Automated mechanisms (eg. Security Information and Event Management (SIEM) system), which correlate all network and system alerts and any other anomalous activity across its business units to detect multi-faceted attacks, shall be established;

(d) Anti-malware solutions shall be implemented so as to prevent malware attacks by scanning all incoming data to prevent malware from being installed and infecting a system;

(e) Multi-layered boundary defences shall be incorporated into IS systems to efficiently monitor the network traffic and filter the flow of data in and out of the organisation;

[5] Principle of least privilege refers to granting a user or a process only those privileges or access to the specific data, resources and applications that are/is necessary for intended function or to complete a required task.

[6] Privileged accounts refer to a user account that has more privileges than ordinary user e.g. Administrator level accounts. Such user may be able to install or remove software, upgrade the operating system, or modify system or application configurations. They might also have access to files that are not normally accessible to standard users.

(f) Network segmentation shall be made based on role, location and environment (production, testing, development, etc.) to segregate systems and data of varying criticality; and

(g) Whitelisting solutions shall be in place to ensure that only permitted applications and services with validated needs are running. Whitelisting of ports may also be ensured.

**16. Application Security Life Cycle (ASLC)**

(a) The PSO shall follow a 'secure by design' approach such as Secure-Software Development Life Cycle (S-SDLC) for design and development of products / services and ensure that no security weaknesses are introduced during the build process.

(b) The PSO shall implement a multi-tier application architecture, that ensures segregation of database layer from other layers, while developing digital payment products and services.

(c) The ASLC guidelines shall apply to procured products / services as well. Further, the PSO shall have an escrow arrangement for the source code of applications procured from third-party vendors, to ensure continuity of services.

**17. Security Testing**

(a) The PSO shall ensure that all its applications are subjected to rigorous security testing, such as source code review, VA, PT, etc., through qualified agencies at adequate frequency in authenticated mode.

(b) If the source code is not owned by the PSO, it shall obtain a certificate from the application developer stating that the application is free of vulnerabilities, malwares and any covert channels in the code.

(c) Deficiencies reported in the security testing shall be resolved in a time bound manner. Any recurring observation shall necessarily be reported to the Board sub-committee along with detailed analysis for recurrence and resolution.

**18. Vendor Risk Management**

The PSO shall be guided by the Framework for Outsourcing of Payment and Settlement-related Activities by PSOs issued by RBI vide circular dated August 03, 2021 (updated from time to time).

(a) The PSO shall put in place necessary security controls for preventing infiltration into its network from vendor environments.

(b) The PSO shall adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and processing, storage and usage of data and also ensure compliance by their vendors.

(c) The PSO shall obtain certified assurance of the vendor's cyber resilience capabilities.

**19. Data Security**

(a) The PSO shall put in place a comprehensive data leak prevention policy for confidentiality, integrity, availability and protection of business and customer information (both in transit and at rest) in respect of data available with it or at vendor managed facilities, commensurate with the criticality and sensitivity of the information held / transmitted.

(b) The PSO shall develop and implement an Information Security Management System (ISMS) based on applicable standards.

(c) Application and database security controls shall focus on secure handling, storage and protection of data, in particular, Personally Identifiable Information (PII). Data in transit and rest shall be secured though either data or channel encryption or both.

(d) The PSO storing card (debit / credit / prepaid) data shall adhere to PCI-DSS guidelines and obtain PCI-DSS certification.

**20. Patch and Change Management Life Cycle**

(a) The PSO shall put in place a documented policy and process to identify and implement patches to technology and software assets released by OEMs / others.

(b) Security patches shall be applied to the relevant systems and applications within an appropriate time frame from their release. In case of critical patches released to tackle well-known / reported attacks, the PSO shall have a mechanism to apply them immediately.

(c) Any change to system, technology, application, source code, etc., shall be managed using robust change management processes and after ensuring that overall integrity of the IT set-up is not compromised.

(d) Patches and changes shall be implemented in production environment after testing and validating the same in other environments (e.g. development, testing, etc.).

**21. Incident Response**

(a) The PSO shall put in place a Board approved incident response mechanism, which shall include provisions to promptly notify its senior management, relevant employees and regulatory, supervisory and relevant public authorities, of cyber incidents.

(b) Response strategies shall incorporate readiness to meet various incident scenarios based on situational awareness and potential impact, consistent communication and co-ordination with stakeholders.

(c) Post-incident analysis, including forensic analysis (wherever necessary), shall be conducted to determine the impact and root cause of incidents. Adequate measures shall be taken to avoid recurrence of similar incidents.

(d) Any unusual incident, including those involving cyber-attacks, outage of critical system / infrastructure, internal fraud, settlement delay, etc., shall be reported to RBI in the Incident Reporting Format (**Annex 1**) within 6 hours of detection. Indicative list of types of incidents to be reported is in **Annex 2**. Any cyber security incident shall also be reported to CERT-In.

**22. Business Continuity Plan (BCP)**

(a) The PSO shall develop a BCP based on different cyber threat scenarios, including extreme but plausible events to which it may be exposed. It shall be reviewed at least once a year and include a comprehensive cyber incident response, resumption and recovery plan, to manage cyber security events or incidents.

(b) The BCP shall be designed to enable rapid recovery from any adverse event and facilitate safe resumption of critical operations aligned with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) while ensuring the security of processes and data.

(c) The PSO shall strive to achieve near-zero RPO.

(d) The PSO shall set up a Disaster Recovery (DR) facility in a different geographical area than the Primary Data Centre (PDC). There shall be a defined methodology for reconciliation of data so as to ensure that there is no data loss while resuming operations from the DR.

(e) DR drills shall be conducted on a half-yearly or more frequent basis. Any divergence from the RTO and RPO shall be analysed and the deficiency be rectified on urgent basis.

**23. Application Programming Interfaces (APIs)**

(a) To safeguard applications against risks emanating from insecure APIs, the PSO shall put in place, inter-alia, the following measures:

(i) Authentication and Authorisation – Establish identity of the communicating applications;

(ii) Confidentiality – Ensure that the message content is not tampered with;

(iii) Integrity – Resources are reliably transferred; and

(iv) Availability and Threat Protection – APIs are available when needed; anomalous[7] activities identified and mitigative action taken.

(b) The PSO shall adhere to relevant standards and globally recognised frameworks on API security.

**24. Employee Awareness / Training**

(a) The PSO shall arrange for periodic repeated training and awareness programs on information security issues for its employees and vendors managing its information assets.

(b) A system of periodic evaluation of cyber security awareness amongst employees shall be operationalised. Employees with an awareness level below a benchmark score may be restricted / prohibited from accessing information assets.

(c) Board members and key senior management personnel shall be provided training and sensitised on information security and cyber risks.

**25. Other Security Measures**

(a) The PSO shall ensure that all payment transactions, including cash withdrawals, involving debit to the account conducted through electronic modes (bank accounts / debit cards / credit cards / PPIs, etc.) are permitted only by validation through multi-factor authentication, except where explicitly permitted / relaxed.

(b) The PSO shall equip its servers with adequate security measures so that unauthorised / spoofed transactions are not done and the authentication process is robust, secure and centralised.

(c) The PSO shall put in place a fraud monitoring solution to identify suspicious transactional behaviour and generate alerts.

(d) The PSO shall appoint a dedicated nodal officer(s) to function on 24x7x365 basis for instant resolution of unauthorised / fraudulent transactions reported by customers and also to facilitate prompt response to Law Enforcement Agencies (LEAs).

(e) The PSO shall put in place a mechanism to capture, analyse, store and archive audit logs in a systematic manner. Log messages shall provide relevant information to uniquely identify the user that initiated an action, the action and parameters of that particular action. Access to log data shall be provided on a controlled basis. Audit logs shall be preserved for a period of at least five years.

[7] Activity that is sufficiently different than historical activity.

(f) The PSO shall ensure that the payment architecture operated by them is robust, scalable and commensurate with the transaction volumes; this shall be reviewed by the sub-committee of the Board.

(g) The PSO shall employ secure mail and messaging systems to ensure that inbound and outbound traffic through mail, messages or any other media are secure.

(h) The PSO shall subscribe to anti-phishing / anti-rogue app services for identifying and taking down phishing websites / rogue applications.

(i) The PSO shall, either directly or through its participants and service providers, continuously create public awareness on precautionary measures to safeguard against frauds and cyber threats while using digital payment products.

## Section IV
## Digital Payment Security Measures / Controls

In addition to the extant instructions applicable to PSOs for digital payment transactions, the following instructions shall also be applicable.

**26.** The PSO shall facilitate its members / participants have mechanisms for online alerts based on various parameters such as failed transactions, transaction velocity, as well as in case of new account parameters (eg., excessive activity), time zone, geo-location, IP address origin (in respect of unusual patterns, prohibited zones / rogue IPs), behavioural biometrics, transaction origination from point of compromise, transactions to mobile wallets / mobile numbers / VPAs on whom vishing or other types of fraud are registered / recorded, declined transactions, transactions with no approval code, etc.

**27.** While sending SMS / e-mail alert to customers, either by PSO or payment system participants, the following shall be ensured –

(a) Bank account number / card number / other confidential information are redacted / masked to the extent possible.

(b) Online payment transactions shall mention merchant name (not the payment gateway / aggregator) and amount; for fund transfers, name of the beneficiary and debit amount. The PSO shall ensure that the name is taken from the system of the entity maintaining the beneficiary account.

(c) In cases where the OTP is a factor of authentication, the PSO shall ensure that the OTP is mentioned at the end of the notification message and the message shall also refer the specific transaction.

**28.** The PSO shall provide a facility on its mobile application / website that would enable customers, with necessary authentication, to identify / mark a fraudulent transaction for seamless and immediate notification to the issuer of payment instrument. It shall also ensure facilitation of such mechanism by the system participants.

**Mobile Payments**

**29.** The PSO providing / facilitating / processing mobile payment services / transactions shall comply with the following security practices and risk mitigation measures and shall also ensure that the participants in its payment system comply with these instructions:

(a) PSO shall put in place a mechanism to ensure that the mobile application is free from any anomalies or exceptions for which the application was not programmed.

(b) The PSO shall ensure that an authenticated session, together with its encryption protocol, remains intact throughout an interaction with the customer. In case of any interference or if the customer closes the application, the session shall be terminated, and the affected transactions resolved or reversed out.

(c) The PSO shall ensure device binding[8] / finger printing of mobile applications with the device and SIM. In case the mobile application remains unused beyond a policy determined specified period, the PSO shall ensure device binding is performed again.

(d) The PSO shall ensure that an online session on mobile application is automatically terminated after a fixed period of inactivity and customers are prompted to re-login.

(e) The PSO shall, where applicable, set down the maximum number of failed log-in or authentication attempts after which access to the mobile application is blocked. There shall be a secure procedure to re-activate the access to blocked product / service. The customer shall be notified for failed log-in or authentication attempts, immediately.

(f) The PSO shall put in place a control mechanism, to identify any presence of remote access applications (to the extent possible) and prohibit access to the mobile payment application while the remote access is live.

(g) Whenever there is a change in registered mobile number or email ID linked to the payment instrument there shall be a cooling period of minimum 12 hours before allowing any payment transaction through online modes / channels.

[8] The device binding shall be preferably implemented through a combination of hardware, software and service information.

**Card Payments**

**30.** The PSO shall ensure that terminals installed at merchants for capturing card details for payments or otherwise are validated against the PCI-P2PE program; PoS terminals with PIN entry installed at the merchants for capturing card payments (including the double swipe terminals) shall be approved by the PCI-PTS program.

**31.** The card networks shall facilitate implementation of transaction limits at card, Bank Identification Number (BIN) as well as at card issuer level. Such limits shall mandatorily be set at the card network switch itself. The card networks shall institute an alert mechanism on a 24x7x365 basis, to be triggered to the card issuer in case of any suspicious incident. Card networks shall ensure that card details of the customers are stored in an encrypted form at any of their server locations as well as their vendor(s)' locations, systems and applications. They shall also ensure that processing of the card details in readable format is performed in a secure manner.

**Prepaid Payment Instruments**

**32.** PPI issuers are encouraged to communicate OTP and transaction alerts with users in a language of their choice, including vernacular languages.

**33.** The PPI issuers – banks and non-banks – shall put in place suitable cooling period for funds transfer and cash withdrawal after such funds are electronically loaded on to the PPI.

## Acronyms

| | |
|---|---|
| API | Application Programming Interface |
| ASLC | Application Security Life Cycle |
| ATM | Automated Teller Machine |
| AUP | Acceptable User Policy |
| BCM | Business Continuity Management |
| BCP | Business Continuity Plan |
| BIN | Bank Identification Number |
| CCMP | Cyber Crisis Management Plan |
| CERT-In | Indian Computer Emergency Response Team |
| CISO | Chief Information Security Officer |
| DR | Disaster Recovery |
| EoLS | End of Life support |
| IDRBT | Institute for Development and Research in Banking Technology |
| IP | Internet Protocol |
| IS | Information System |
| ISMS | Information Security Management System |
| IT | Information Technology |
| KPI | Key Performance Indicator |
| KRI | Key Risk Indicator |
| LEA | Law Enforcement Agency |
| NCIIPC | National Critical Information Infrastructure Protection Centre |
| OEM | Original Equipment Manufacturer |
| OTP | One Time Password |
| PCI | Payment Card Industry |
| PCI-DSS | Payment Card Industry-Data Security Standard |
| PCI-P2PE | Payment Card Industry-Point to Point Encryption |
| PCI-PTS | Payment Card Industry-PIN Transaction Security |
| PDC | Primary Data Centre |
| PIN | Personal Identification Number |
| PoS | Point of Sale |
| PPI | Prepaid Payment Instrument |
| PSO | Payment System Operator |
| PSS | Payment and Settlement Systems |
| PT | Penetration Testing |
| RBI | Reserve Bank of India |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SDLC | Software Development Life Cycle |
| S-SDLC | Secure-Software Development Life Cycle |
| SIEM | Security Information and Event Management |
| SIM | Subscriber Identification Module |
| SMS | Short Message Service |
| SOC | Security Operations Centre |
| VA | Vulnerability Assessment |
| VPA | Virtual Payment Address |
| WLAO | White Label ATM Operator |