Information Security and Cyber Security Policy

Level 1 Policy

Document Information

Document Owner	InfoSec Team
Document Approver	Information Security committee
Version	2.0
Effective Date	28-05-2024
Distribution	WeRize's Internal Team, Employees, Customers, Vendors

Version History					
Version	**Date**	**Author**	**Reviewer**	**Approver**	**Document changes**
1.0	21-09-2020	Kiran	Aditya Veer Singh	Information Security committee	Initial document release
1.1	28-04-2021	Kiran	Aditya Veer Singh	Information Security committee	Minor changes as part of annual review
1.2	22-04-2022	Ronak	Aditya Veer Singh	Information Security committee	Minor changes as part of annual review, changed MoneyOnClick to WeRize as part of rebranding activity
1.3	24-05-2023	CyRAACS	Aditya Veer Singh	Information Security committee	Additional of RBI Master Direction controls
2.0	28-05-2024	CyRAACS	Aditya Veer Singh	Information Security committee	Change are made according to ISO 27001:2022

Contents

1. Purpose

The purpose of this document is to ensure that adequate controls are implemented for Wortgage Technologies Private Limited hereinafter called as WeRize, to ensure information is appropriately available, accurate, secure, and complies with legislative requirements. This policy provides management direction and support for information security across the organization.

2. Abbreviations & Definitions

2.1. Abbreviations

Abbreviation	Description
Covered Persons	Employees, Consultants, Temporary employees

2.2. Definitions

Information Security: Preservation of confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

3. Scope

The scope of Information Security policies applies to all Covered Persons and covers all IT infrastructure including cloud environment, networks, applications, hosts, databases in use. Customer Information, organizational information, supporting IT systems, processes and people that are generating, storing, and retrieving information are important assets of WeRize.

This Information Security Policy addresses the information security requirements of:

Confidentiality: Protecting sensitive information from disclosure to unauthorized individuals or systems

Integrity: Safeguarding the accuracy, completeness, and timeliness of information

Availability: Ensuring that information and vital services are accessible to authorized users when required

Authenticity: Ensuring that the data, transactions, communications, or documents (electronic or physical) are genuine.

Other principles and security requirements such as Non-repudiation, Identification, Authorization, Accountability, and audit ability are also addressed in this policy.

4. Ownership

The Information Security committee which consists of Executive Management is the owner of this policy and ultimately responsible for information security. This policy shall be ratified by the Information Security committee to form part of its policies and procedures on expected standards on conduct and behavior. The Information Security Policy Documentation set shall be maintained by Information Security team and individual policies may be delegated to respective function owners/heads. This policy and subsidiary policies shall be reviewed and updated regularly at least on an **annual** basis to ensure that all remains appropriate in the light of any relevant changes to the law, organizational policies, or contractual obligations. It is the responsibility of all employees to ensure that they conduct their business in accordance with this policy. The selected policies as defined by the RBI IT Directives will be approved by the Board of Directors.

5. Information security policy

- Scope and boundaries of ISMS must be defined and reviewed at least annually considering the business, contractual requirements, and legal obligations. Any exclusion from the ISMS scope shall be justified and documented.
- Pre-defined and systematic approach to identify business critical processes and corresponding information assets, risk assessment, evaluation of risk treatment potions, criteria to accept risks and to identify the acceptable risk levels shall be followed as mentioned in the risk management methodology.
- A statement of applicability (SOA) shall be prepared and updated based on the current applicable controls.
- Security policies and procedures shall be developed/ updated/ modified to address selected controls and for their implementation.
- Compliance and security teams shall be formed to implement, operate and maintain the ISMS at WeRize
- Compliance and security leader shall be responsible for implementing, operating and maintaining the ISMS at WeRize.
- Selected controls based on the SOA must be implemented after developing a risk treatment plan. The actions to be taken by the management, resources required, responsibilities and the period for implementation should be identified in the implementation plan.
- Suitable measures for effectiveness of controls or group of controls shall be established for their evaluations.
- Security awareness training programs shall be conducted on a quarterly basis i.e. for new joiners during induction and for rest once in a year.
- Procedures for prompt information security incident detection, reporting, response and escalation shall be implemented.
- Internal ISMS audit shall be carried out at least once in a year.
- All policies and procedures need to be reviewed annually, or in the event of a change.
- Effectiveness of the ISMS shall be measured every year from the inputs of internal audits, security audits, incidents, control effectiveness measurements, suggestions and feedback from all interested parties.
- Risk assessment should be conducted at least once a year or in an event of major change in the information processing or information storage facilities or change in regulatory requirements.
- Record of actions and events affecting ISMS shall be maintained.
- Identified improvements in the ISMS shall be implemented.
- Corrective actions shall be taken to rectify weakness in control environment and any future non-conformity.
- Compliance and Security Team shall ensure that the ISMS improvements achieve the information security objectives

6. Information Security Governance

Information security governance consists of leadership, organizational structures and processes that protect information and mitigation of growing information security threats Critical outcomes of information security governance include:

1. Alignment of information security with business strategy to support organizational objectives
2. Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
3. Management of performance of information security by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved
4. Optimization of information security investments in support of organizational Objectives

7. Responsibilities

Role	Responsibility	Authorities
IT Strategy Committee	1. Provide IT insights to board and act as subject matter expert 2. Monitor strategic IT plans 3. Monitor enterprise resource availability to support IT initiatives 4. Understand, Communicate, Mitigate IT risk (may also be coordinated with a Risk or Compliance Committee) 5. Monitor the significant changes in the exposure of information assets to major threats 6. Responsible for overall development and management of information technology assurance measures and its compliance to the policies and procedures	1. Approve IT strategic plans, oversee major initiatives, and allocate resources 2. Review and monitor the incidents and commission the corrective actions
Management	1. Approve policies related to information security function 2. Ownership for implementation of board approved information security policy Ownership for establishing necessary organizational processes for information security Ownership for providing necessary resources for successful information security Ownership for establishing a structure for implementation of an information security program	Provide necessary resources for implementing Information Security.
Information Security Committee	1. Developing and facilitating the implementation of information security policies, and procedures to ensure that all identified risks are managed within a bank's risk appetite. 2. Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving procedures. Supporting the development and implementation of a bank-wide information security management program 3. Reviewing the position of security incidents and various information security assessments and monitoring activities across the bank 4. Reviewing the status of security awareness programs 5. Assessing new developments or issues relating to information security 6. Requirement for generating effective metrics for measuring	1. Conduct regular ISC meetings. 2. Approve Information Security Policy. 3. Manage Information Security Incidents.

	performance of security control 7. Reporting to the Management on information security activities 8. Conducting regular ISC meetings (at least annually) and maintenance of Minutes of Meeting	
Information Security team	1. Establishing, implementing, monitoring, reviewing, maintaining, and improving Information Security Management System 2. Reviewing the security policies/procedures and suggesting improvements 3. Coordinating the ISC meetings 4. Providing consultative inputs to the ISC on security requirements 5. Coordinating information Security initiatives in the organization 6. Driving and monitoring the ISC directives in the organization 7. Updating ISC about IS initiatives, issues, and incidents 8. Facilitating and Conducting risk assessments of Information Assets used and recommend mitigation controls 9. Promote security awareness amongst employees, customers, and partners.	1. Improving Information Security Management System. 2. Review Information Security policies.
Function/ Business Heads	1. Heads of Business / function units are ultimately responsible for managing information risk in their respective business as part of their wider risk management responsibilities 2. Nominate Asset owner 3. Providing resources and support to the Asset Owners for information security implementation in the business unit 4. Assist in Implementing policies, procedures, and control techniques identified in the information security program. 5. Ensuring terms of service and other contractual agreements satisfy the security and privacy requirements applicable for information systems	1. Manage information risk in respective business. 2. Provide resources for information security implementation.
The Board of directors	1. Responsible for the implementation and compliance of the security related to that information as identified in the Information Security Policy. 2. Coordinate the design and implementation of the Information Security Program with the Chief Information Security Officer 3. Review existing Information Security Policies, Standards, and Processes & Procedures to ensure that they meet regulatory requirements and current standards. 4. Approve changes to Information Security Standards and Processes & Procedures to comply with the organization Policy	1. Approval authority for policies deployment/changes 2. Risk review/acceptance (With respect to ISMS best practices at the org level)

	5. Review and approve exceptions to Information Security Policies, Standards, and Processes & Procedures.	

8. Policies

Information Security policies have been framed based on a series of security principles. All the Information Security policies and their need have been addressed below:

8.1. Information and Cybersecurity Policy

8.2. Acceptable Usage Policy

1. WeRize proprietary information stored on electronic and computing devices whether owned or leased by WeRize, the employee or a third party, remains the sole property of WeRize. Covered Persons1 must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard
2. Employees have a responsibility to promptly report the theft, loss, or unauthorized disclosure of proprietary information
3. Employees may access, use, or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
5. For security and network maintenance purposes, authorized individuals may monitor equipment, systems, and network traffic at any time, per Information Security's Audit controls.
6. WeRize reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy
7. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
8. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.
9. Postings by employees from a WeRize email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of WeRize, unless posting is in the course of business duties.
10. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware. *Refer: Acceptable Usage Policy*

8.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities.

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by WeRize.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which WeRize or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent offers of products, items, or services originating from any account. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
9. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network, or account.
11. Introducing honeypots, honeynets, or similar technology on the network.
12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
14. Providing information about, or lists of, employees to parties outside WeRize.
15. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
16. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
17. Unauthorized use, or forging, of email header information.
18. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
19. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
20. Use of unsolicited email originating from within 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via WeRize's network.
21. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
22. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by WeRize 's Confidential Information policy when engaged in blogging.

8.4. Information Handling Policy

This policy sets out the need to define classes of information handled by the Organization and the requirements on the labeling, storage, transmission, processing and disposal of each. Requirements include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups)

Information Classification

Classification	Description	Protection required	Examples
Public	These documents may be viewed by any member of the public. No Personal Data, or disclosure of Personal Data would be reasonably expected by the Subject.	This information is accessible in public domain	Press Releases, Freedom of Information Responses, Information within the Publication Scheme (including Policies & Procedures), Information published to the corporate website
Internal	Access generally limited to internal employees (low risk). Contains Personal Data, but disclosure would not normally be reasonably be expected by the Subject.	This information should be accessible to the organization employees whilst it is required for business purposes Backup requirements will need to be considered in relation to the importance of the information	Internal policies, procedures, Internal communications
Restricted	Access limited to those with a requirement to view (medium risk). Contains Personal Data, but disclosure would not reasonably be expected by the Subject.	This information should be accessible to the organization employees whilst it is required for business purposes Backup requirements will need to be considered in relation to the importance of the information	Employee records, Contracts, Reserved committee minutes, Financial information (not disclosed in Financial Statements), databases and spreadsheets containing personal data, Personal data within email messages.
Confidential	Access limited to a select group of individuals (high risk). Contains Special Categories of Personal Data	This information requires security measures, controlled and limited access and protection from corruption Backup requirements will need to be considered in relation to the importance of the information	Customer data, Passwords, Security Sensitive research material, Disciplinary proceedings, Legally privileged information, Occupational Health records, Email messages containing special categories of personal data.

Information Handling and Disposal

Domain	Public	Internal	Restricted	Confidential
Data storage	Can be stored on	Information must be	Information must be	Information must be

and access	any device and on the internet. No restrictions on printing and copying this data, subject to copyright restrictions.	held within organization systems. Paper documents must not be left unattended. Appropriate controls should limit access to only those members of the Organization that require it.	held within organization systems. Paper documents must not be left unattended. Data should only be placed in areas with restricted access. Data held within information systems must be controlled as described in the User access Management Policy.	held within organization systems. Paper documents must not be left unattended. Data should only be placed in areas with restricted access. Data held within information systems must be controlled as described in the User access Management Policy.
Data Transfer/sharing	Data may be freely transmitted without restriction.	Data may be placed on the WeRize managed systems and sent via internal email with appropriate controls on access. Data may be sent via internal email with appropriate care in addressing. Data should not generally be transferred to any non-organization managed mobile devices	Where possible, data within information systems should be accessed within that system and not exported or shared. If transfer or sharing is required then appropriate controls must be used to safeguard the data. Data should only be transferred to encrypted mobile devices. Encryption must be used when emailing data to external recipients. Items sent by internal and external mail should be placed in sealed envelopes.	Where possible, data within information systems should be accessed within that system and not exported or shared. If transfer or sharing is required then appropriate technology, such as encryption, must be used to safeguard the data. Data should only be transferred to encrypted mobile devices. Hard copies of documents should be hand delivered internally. External mail should be signed for and double enveloped.
Document marking	None.	'INTERNAL' on the document cover sheet (if applicable) and on each page.	'RESTRICTED' on the document cover sheet (if applicable) and on each page.	'CONFIDENTIAL' on document coversheet (if applicable) and on each page.
Disposal	No restrictions.	Paper documents must be crosscut shredded. Electronic media must be securely wiped as per NIST 800-88 Guidelines for Media Sanitization	Paper documents must be crosscut shredded. Electronic media must be securely wiped as per NIST 800-88 Guidelines for Media Sanitization	Paper documents must be crosscut shredded. Electronic media must be securely wiped as per NIST 800-88 Guidelines for Media Sanitization

8.5. Email Security policy

1. All email on the (company) information systems, including personal email, is the property of (company) . As such, all email can and will be periodically monitored for compliance with this policy.
2. Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members, such as between a producer and an account representative. In all other cases, no user is authorized to open or read the email of another without the express consent of senior management (i.e., CEO, COO, or VP of Function Head).
3. Email is provided to the users of (company) primarily to enhance their ability to conduct business.
4. The maximum size of any individual incoming email message will be 20 MB.
5. Terminated employees will have all email access immediately blocked.
6. Auto forwarding of emails will be blocked for users
7. All mail communications will be over TLS 1.2 Encryption protocol
8. Use of profane, inappropriate, pornographic, slanderous, or misleading content in email is prohibited.
9. Use of email to spam (i.e., global send) is prohibited. This includes the forwarding of chain letters.
10. Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, color, sex, age, disability, national origin or any other category.
11. Use of email to send unprofessional or derogatory messages is prohibited.
12. Forging of email content (i.e., identification, addresses) is prohibited.
13. All outgoing email will automatically include the disclaimer statement
14. 'This email is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any review, dissemination, copying, printing, or other use of this email by persons or entities other than the addressee is prohibited. If you have received this email in error, please contact the sender immediately, and delete the material from your computer'.
15. Internet Usage policy.
16. Internet access is provided to WeRize employees to conduct WeRize business. While these resources are to be used primarily for WeRize business, the company realizes that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites
17. Internet activity will be monitored for misuse.
18. Internet activities that can be attributed to a WeRize domain address (such as posting to newsgroups, use of chat facilities and participation in email lists) must not bring disrepute to WeRize with controversial issues (i.e., sexually explicit materials).
19. Internet use must not have a negative effect on WeRize operations. Users will not make unauthorized purchases or business commitments through the Internet. Internet services will not be used for personal gain.
20. Internet users will make full attribution of sources for materials collected from the Internet. Plagiarism or violation of copyright is prohibited.
21. Release of WeRize proprietary information to the Internet (i.e., posting information to a newsgroup) is prohibited.
22. All Internet users will immediately notify the IT team of any suspicious activity.
23. All remote access to the WeRize internal network through the Internet will be encrypted and authenticated in a manner authorized by the IT team. Refer: Communication policy

8.6. Cloud Security

1. Virtual private cloud or a similar technology must be used when a secured private or isolated network is required within the cloud environment.

2. Network devices/Firewall in private cloud environments that are owned and operated by WeRize must be configured to send logs to a centralized log collector. Refer: Cloud Security Policy

8.7. Communication Management

1. All users of WeRize email systems must be provided pre-approved email access based on defined role matrix.
2. Usage of email shall be consistent with policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
3. No non-business-related newsgroup should be added to the allotted WeRize e-mail address book. *Refer: Communication Management Policy*

8.8. Anti-Malware policy

This policy is designed to help prevent infection to WeRize Information systems by computer viruses and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

1. All information systems connected to the WeRize network (herein referred to as "the network") or networked resources must have anti-virus software installed, configured so that the virus definition files are current, routinely, and automatically updated, and the anti-virus software must be actively running on these devices.
2. All files on computer devices will be scanned periodically for viruses. The IT team will establish a schedule for automatically scanning the devices within its control.
3. The anti-virus product shall be operated in real time on all servers and user computers. The product shall be configured for real time protection. The anti-virus library definitions shall be updated at least once per day.
4. Anti-virus scans shall be done a minimum of once per week on all user-controlled workstations and servers.
5. If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the network until the infection has been removed. This will be done under the direction of the IT / Technology Head and the Information Security team.
6. WeRize allows employees to use personally owned computers for business purposes and must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
7. All employees are responsible for taking reasonable measures to protect against virus infection.
8. Employees must not attempt to either alter or disable anti-virus software installed on any computer. *Refer: Anti- Malware Policy*

8.9. Data Retention and Disposal Policy

1. WeRize is bound by various obligations regarding the data that WeRize process or control. These obligations include how long WeRize can retain Data and when and how WeRize can destroy it. The obligations can arise from industry standards, local laws, or regulations or from contracts and promises that WeRize make to employees, customers, goods and service providers and partners.
2. Further, WeRize can be involved in unpredicted events such as litigation or business disaster recoveries that require WeRize to have access to the original Data to protect WeRize's interests or those of employees, customers, goods and service providers and partners.
3. As a result, Data needs to be archived beyond its active use. A contract can, for example, expire after two years but other Data can, by law, need to be retained for a longer period. Refer: Data Retention policy

8.10. Asset Management policy

1. Information assets should be defined and documented in an Asset Inventory that is easily maintainable e.g., a spreadsheet, containing useful information about each information asset identified including:

a. Asset ID
b. Description or descriptive name.
c. Location(s) of the information asset.
d. Asset owner with responsibility for handling the information or managing the information asset.
e. The type(s) of information stored or processed.
f. Origin or custodian of the information stored or processed.
g. The importance of the information stored or processed.
h. Any special or non-standard security measures required.

2. This document should be reviewed regularly by the information custodian. as identified by their position. The list of information custodians by job role is set out in the Information Custodians section.
3. Information assets include, but are not limited to, data in databases and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information
4. Information assets should be classified according to sensitivity of the data, criteria for which are set out in the Data Classification section:
   a. Confidential
   b. Restricted
   c. Internal
   d. Public
5. Labeling of output should reflect the most sensitive information held within it and carry an appropriate and prominent label within the output e.g., printed headers on paper output
6. Periodically reviewing and updating the list of important information assets is recommended. Performing at least a basic non-technical review of how the information involved is handled may help to identify one of these common problems that can lead to a security incident. *Refer: Asset Management Policy*

8.11. Access Management Policy

1. **Role based Access Control**:
   Access to information should be based on well-defined user roles (system administrator, user manager, application owner etc.), WeRize shall avoid dependence on one or few persons for a particular job. There should be clear delegation of authority for right to upgrade/change user profiles and permissions and key business parameters (e.g., interest rates) and the same should be documented.
2. **Segregation of functions:**
   WeRize shall maintain segregation of the duties of the Security Officer/Group (both physical security as well as cyber security) dealing exclusively with information systems security and the Information Technology. WeRize shall ensure that the information security function is adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. and a clear segregation of responsibilities relating to system administration, database administration and transaction processing shall be maintained. Refer: Access Management Policy

8.12. Password Policy

1. User must use separate, unique password for each of their work-related accounts. User must not use any work-related passwords for their own, personal accounts.
2. All the default passwords must be changed immediately upon installation and configuration of the systems or networking devices, and it must follow the password complexity criteria. *Refer: Password Policy*

8.13. Maker-Checker:

For all finance related transaction within the organization shall implement maker-checker process i.e., there should be at least two individuals necessary for processing a transaction.

8.14. Human Resource Security Policy

1. **Personnel Security:**
   Personnel with privileged access like system administrator, cyber security personnel, etc should be subject to rigorous background check and screening. *Refer: Human Resource Security Policy*

8.15. Cryptography Control Policy

1. Use of cryptographic controls

1.1. Cryptographic controls shall be used to protect the confidentiality and integrity of information based on the associated risk. The policy shall address:

- required encryption levels based on the associated risk of the information
- the use of encryption on removable media devices
- the use of encryption for information in transit
- key management, including protection, recovery, and revocation
- roles and responsibilities, including responsibilities over implementation and ongoing management
- implementation process
- contractual, legal, and regulatory requirements

2. Digital Certificates

WeRize shall use digital signatures for verifying the authenticity and integrity of digital documents or messages and increase the trustworthiness of their communications by authenticating the communicating parties. For digital certificates, WeRize shall verify the validity of the certificate and its issuing organization prior to accepting the certificate and trusting the according user. Certificates and their belonging secret keys shall not be shared or reused.

All non-public and sensitive information (including credentials) shall be stored in a secured manner and encrypted whenever this information is stored outside of WeRize access control. For credentials, encryption is always mandatory in storage, even on system under WeRize access control. The transmission of non-public information (including credentials) shall not happen in clear text. The usage of a VPN or end-to-end encryption is mandatory. This especially includes the distribution and exchange of secret keys that shall not under any circumstances be transmitted unencrypted. WeRize shall ensure that the Digital Signature Certificate procurement and management is centralized, and their use is tracked.

The Digital Signature Certificate management procedure shall be documented and periodically reviewed. Compromised credentials, both certificates and passwords shall be revoked / disabled immediately if compromised. Every user is obliged to immediately report the compromise of credentials whenever detected. Digital certificates which are still needed shall also be replaced prior to expiration to avoid disruption in communication.

The technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to end encryption.

WeRize team managing the Digital Signature Certificate shall ensure:

- correct addressing and transportation of the message

- reliability and availability of the service
- legal considerations, for example requirements for digital signatures
- Maintaining a centralized inventory of all the certificates being used by the organization and ensuring their validity
- obtaining approval prior to using external public services such as instant messaging, social networking, or file sharing
- stronger levels of authentication controlling access from publicly accessible networks
- Ensuring that service providers receive, validate, and transmit identification and authentication information

3. **Key management**

   WeRize shall implement the usage of Public Key Infrastructure (PKI) to ensure confidentiality of data, access control, data integrity, authentication, and nonrepudiation. Refer Document: Cryptography Policy

8.16. Social Media Policy

1. Employees need to know and adhere to the WeRize Code of Conduct & policies when using social media
2. Employees should be aware that WeRize may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to WeRize, its employees, or customers
3. Controls such as encryption and secure connections shall be prevalent to mitigate risks related to social media. *Refer: Social Media Policy*

8.17. VPN Policy

1. WeRize shall monitor and control remote access to its network.
2. Remote access to the WeRize Network shall require Multi Factor Authentication or additional access control measures approved by WeRize Security.
3. WeRize shall approve Virtual Private network (VPN) connectivity or connectivity through a secured sockets layer or transport layer security. *Refer: VPN Policy*

8.18. Vulnerability Management Policy

1. WeRize vulnerability management policy covers IT infrastructure including cloud environment, networks, applications, hosts, databases in use to cover under VAPT and remediate reported vulnerabilities within defined timeframes.
2. All systems are required to undergo vulnerability assessment of all of their networked computing devices on a quarterly basis either by internal assessor or third party assessor.
3. At a minimum, systems shall run authenticated scans from the enterprise class scanning tool on a quarterly basis against all networked computing devices within their control.
4. The approved enterprise vulnerability scanning tool must be used to conduct the scans unless otherwise authorized (see References).
5. Scans shall be performed during hours appropriate to the business needs of the entity and to minimize disruption to normal business functions.
6. Data from scans are to be treated as Confidential, i.e., Level 2, consistent with WeRize Information Classification policy.

7. Remediation Management: Vulnerability reports provide system owners and administrators the opportunity to understand the potential risk to which their systems may be exposed, and to take proactive steps to address the identified vulnerabilities. *Refer: Technical Vulnerability Management Policy*

8.19. Mobile Device and Teleworking Policy

Mobile devices are provided to assist Employees to conduct business efficiently and effectively. This equipment, and any information stored on mobile devices, must be recognized as valuable organizational information assets, and safeguarded appropriately.

For the purpose of this guidance, mobile devices are classified as any device holding data which is likely to be carried from place to place and includes:

- Laptop computers, tablets, handheld computers (especially PDAs)
- USB Pen drives
- Mobile phones (especially smartphones)
- CD/DVD ROMs
- portable hard drives

These portable devices are more prone to being lost due to the nature of their portability.

All users are required to abide by the following security best practices.

1. Users must not store confidential/sensitive or personal data e.g., info relating to individuals that has been provided by the Organization, on a mobile device without prior authorization from the data owner or custodian. Users may not save data without expressed permission.
2. confidential/sensitive or personal data stored on a mobile device, must be encrypted using a minimum of AES 128/256-bit encryption with a strong key/password of at least 10 characters (see password guidelines).
3. AES 256-bit USB pen drives are available widely and are recommended. Some models will destroy the data after six failed attempts to crack the password. Other secure USB drives with combination locks etc., have been shown to be easy to hack and should be avoided.
4. Any device that pulls email from the WeRize systems e.g., Smartphone, Blackberry, iPhone etc., whether owned by the WeRize or by the individual, must be effectively protected with a system authenticated password.
5. Sensitive or confidential data should, ideally, not be passed by email. Where this is unavoidable, it must be encrypted.
6. Disable Wi-fi and Bluetooth when you don't need them. Not only does this make your mobile device more secure but saves on the battery use. Disabling/enabling these features varies from device to device - your lap-top and Smartphone manuals will contain the details.
7. Avoid accessing or transmitting sensitive/confidential data when connected to public and open wi-fi hot spots during teleworking.
8. When using your laptop in public spaces e.g., on trains, airport lounges, you must take care over what can be seen on your screen.
9. Care should be taken to protect mobile devices from theft while teleworking: Lock laptops, and tablet computers in the boot when parked or traveling by car
10. Don't leave your mobile devices/phone in an unattended state
11. Take extra care and be vigilant in public spaces and on public transport
12. Make sure you lock the office door when leaving equipment unattended
13. All lost or stolen devices that contain confidential, sensitive, or personal data belonging to the WeRize must be reported immediately to the IT/ Information Security team and where appropriate (laptop, phone) to the police.
14. Mobile phone apps represent a new risk from malware and viruses. Downloaded apps can incorporate undesirable code which opens your phone up for hacking. Only buy from dedicated app stores and avoid downloading pirated apps. Be cautious and wary of software downloads and their origins.
15. E-mail concerning business is discoverable under freedom of information and data protection legislation. Therefore, you must take care when writing emails, not to be liable or be derogatory about individuals or

organizations. Always assume that those mentioned in an email are free to read the email if they so wish. Refer: Mobile device Policy and Teleworking Policy.

8.20. Removable Media Policy

Removable media includes below:

- Memory cards (like those used in cameras), USB pen drives etc.
- Removable or external hard disk drives
- Newer Solid State (SSD) drives
- Mobile devices (iPod, iPhone, iPad, MP3 player)
- Optical disks i.e., DVD and CD
- Floppy disks
- Backup Tapes

1. The use of removable media is prohibited within the WeRize environment and access to removable media is provided with appropriate authorization from the Function head and Information Security team.
2. When removable media is used, regularly updated Anti-Virus software should be present on all machines from which the data is taken from and machines on which the data is to be loaded
3. When removable media is used to transport sensitive data, the data on the device must be encrypted to a recommended encryption standard (AES-256)
4. Mobile devices and/or removable storage containing sensitive or highly sensitive data should not be sent off site without prior authorization from function head
5. Removable media used to store sensitive and highly sensitive data shall only be used by staff who have an identified and business need for them
6. Removable media should be physically protected against loss, damage, abuse or misuse when in use, storage and transit.

8.21. Physical Security Policy

The objective of this policy is to provide and ensure controlled physical access and environmental security to information assets and information security assets on the basis of business and security requirements.

1. Access to information processing facilities such as secure location of critical data shall be secured. The access shall be granted on a need basis.
2. The entry and exit of visitors shall be controlled. Before a visitor enters a building, the security guards at the reception desk or gate shall verify the visitor identity using generally accepted credentials (e.g., an Identity Card or Passport). Entry shall be allowed only after notifying the employee to whom the visitor is visiting and verifying the purpose of the visit.
3. Visitors and third-party support services will be escorted to secure areas or sensitive areas only when required following the visitor management process. The access will be monitored all times.
4. Admin team shall be responsible for managing and monitoring CCTV cameras and access doors systems within common areas and Datacenter.
5. All entries to Datacenter shall be recorded and maintained for at least 6 months. All access logs shall record the following details:

a. The date and time of the access attempt.
b. Whether the attempt was successful or not.
c. Where access was granted (which door for example).
d. Who attempted the access.
e. Who modified the access privileges at the supervisor level.

6. Personnel who do not require continuing access to Datacenter shall be escorted by an authorized employee at all times and shall be required to sign a visitor control log.
7. The facilities where sensitive information and critical systems are stored or processed shall be constructed and arranged in a way that they are adequately protected from physical and environmental threats.
8. Hazardous or combustible materials shall be stored securely at a safe distance from a secure area.
9. Security and Safety Department shall observe personnel safety as a high priority and take the necessary steps to ensure a safe workplace.
10. Proper procedures regarding the safe evacuation of areas or buildings in case of fire, flood, earthquake or other disasters shall be developed and documented in order to protect employees and systems.
11. Environmental controls shall be designed and applied to minimize the damage resulting from fire, flood, earthquake, explosion, civil unrest and other forms of natural or human-caused disasters.
12. WeRize facilities shall contain emergency equipment (e.g., emergency lighting, and fire extinguishers) to establish an adequate level of safety for those working within a facility. This equipment shall be inspected on an annual basis in order to ensure their operational capabilities.
13. Areas where the Data Center is located shall have appropriate external and environmental controls in place (e.g., temperature, humidity, dust particle content, atmospheric pressure, electromagnetic radiation, or static electricity) according to the manufacturer's recommendations.
14. Admin team shall be responsible for the physical monitoring of the Datacenter. In particular, the following assets shall be centrally monitored:
    a. Physical access control.
    b. Ventilation and Air-Conditioning.
    c. Emergency power supply (i.e., power generator) and UPS.
    d. Fire detection and suppression systems.
    e. Water detection system.
    f. CCTV.
    g. Racks.

    Since our data centers are part of AWS Cloud and GCP Cloud offerings, they are covered by ISO 27001:2013 which gets renewed regularly .
15. Delivery and loading areas shall be controlled and, if possible, isolated from facilities to avoid unauthorized access or causing destruction to sensitive areas. Security requirements that control delivery and loading area shall include, but not be limited to:

    a. Access to a loading area from outside of office premises shall be restricted to identified and authorized personnel.

    b. The loading area shall be designed in which supplies can be unloaded without delivery staff gaining access to other areas of office premises.
16. All incoming packages to office premises shall be received by reception staff to be inspected. Also, they shall be recorded in a register.
17. Based on information and/or systems classification, equipment shall be protected to reduce risks from environmental threats and hazards; and to reduce the risk of unauthorized access to information.
18. The followings controls shall be considered to secure all critical systems:
    a. Equipment is located in a physically secure location to minimize unauthorized access.
    b. Environmental conditions are monitored for conditions that could adversely affect the operation of computer systems.
    c. System owners need to consider the potential impact of a disaster happening in nearby premises (e.g., a fire in a neighboring building or water leaking from the roof or in floors below ground level or an explosion in the street).
19. Information processing systems will be set up in a way that the risk of damage will be minimized.
20. All sensitive information/ cables will be placed separate from general equipment.
21. Admin team shall provide power protection to ensure the availability of IAU's systems.
22. To achieve continuity of power supplies, the following shall be considered, but not be limited to:

a. Multiple feeds to avoid a single point of failure in the power supply.

b. Uninterruptible Power Supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical systems and business operations. UPS shall be regularly tested, as per vendor's instructions, to ensure reliable functionality.

c. A backup generator is considered when processing and business continuity is required.

23. All critical systems shall be configured to switchover to an alternate power source immediately upon loss of power.
24. Equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided in accordance with equipment manufacturer's specifications.
25. Supporting infrastructure (e.g., air conditioning systems and security alarm systems), where applicable, shall have a dependable and consistent electrical power supply that is free from surges and interference that shall affect operation of the equipment (e.g., power-conditioning strips could reduce the threat of power surges).
26. UPS shall be regularly tested, as per vendor's instructions, to ensure reliable functionality.
27. Equipment maintenance will be carried out by authorized personnel and equipment movement will be authorized after securing information.
28. Equipment, assets or software shall not be taken off-site WeRize without a proper authorization. Where necessary and appropriate, the followings shall be considered:
    a. Personal shall obtain a proper authorization to take equipment off-site.
    b. Equipment is logged out.
    c. Time limits are set.
    d. When returned, equipment is logged back in
29. Admin team function head shall develop appropriate procedures for the followings:

a. Disposal of confidential documents.

b. Destruction of computer equipment that may contain sensitive information.

c. Sanitization (i.e., object reuse) of equipment that might be sold or transferred to another organization.

d. Destruction of various types of media.

30. Storage media (e.g., CD-ROMs, tapes and flash memories) that contains sensitive information that no longer needs to be kept shall be physically destroyed as follows:

a. Rewritable media is erased using a secure procedure (e.g., through multiple overwrites, may be three or more times) to prevent the data from later being scavenged.

b. Paper documents are destroyed using paper shredders.

31. Admin team function head shall maintain disposal records which include the information owner's disposal request and the corresponding department director's approval.
32. Equipment and storage media shall be checked prior to disposal or re-use to ensure that sensitive information and licensed software has been removed or securely overwritten.
33. Destruction of sensitive information captured on storage media shall only be performed after approval has been obtained for the method of destruction using Department of defense (DOD) of degaussing or physical destruction. *Refer: Physical security Policy*

7.21 Network Security Policy

1. The WeRize IT network(s) will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The IT network(s) must also be able to withstand or recover from threats to its availability, integrity and confidentiality.
2. Access to the network resources will be via a secure log-on procedure, designed to minimize the opportunity for unauthorized access.
3. The WeRize operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. All workstations and laptops must be locked if left unattended for a short time. Users failing to comply may be subject to disciplinary action
4. No equipment is to be connected to any IT network without the approval of those that manage/operate the IT network concerned.

5. Security privileges (i.e. 'superuser' or network administrator rights) to the network will be allocated based on the requirements of the user's role.
6. Third party access to the IT network(s) will be controlled; the policy and process for authorization; request; and configuration is detailed in the Third Party Management Policy. This includes a formal contract that covers both security and information governance requirements.
7. All external connections to the core WeRize IT network(s) are to be mediated by appropriate access controls that protect against unauthorized or inappropriate access to the network and/or resources hosted on it. Such mediation will also control access and scan all authorized traffic via appropriate technical measures in order to protect the hosted resources.
8. The IT department will ensure that appropriate maintenance contracts are maintained and periodically reviewed for all core network equipment. All contract details will constitute part of the Technology departments Information Asset register.
9. The IT department is responsible for ensuring that a log of all faults on the core IT network is maintained and reviewed.
10. Documented operating procedures will be prepared for the operation of the network, to ensure its correct, secure operation. Changes to operating procedures must be authorized by the Head of IT.
11. Wherever possible use should always be made of secure IT protocols over insecure legacy protocols i.e. Secure Shell (SSH) rather than 'Telnet', Secure File Transfer Protocol (SFTP) instead of File Transfer Protocol (FTP) where this may not be possible then a risk assessment is to be conducted and documented.
12. For 'core' systems the IT department will ensure that measures are in place to detect and protect the network from viruses and other malicious software.
13. Head of IT is to ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.
14. All potential security breaches on the IT networks must be reported to the Technology security team who will investigate as appropriate. Information Security incidents and weaknesses must be reported in accordance with the requirements of the organization's incident reporting procedure.
15. Head of IT Operations is to ensure that business continuity plans and disaster recovery plans are produced for the IT network. The plans must be reviewed by the Technology departments' Head of IT Operations and tested on a regular basis.
16. IT team shall be trained to understand and support implementation of this policy. The Trust will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

7.22 Incident Management Policy

1. WeRize shall develop and implement processes for preventing, detecting, analyzing and responding to information security incidents. Refer: Incident Management Policy and Procedure

7.23 Logging and Monitoring Policy

1. WeRize shall ensure that audit trails are maintained for IT assets satisfying the business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. Refer: Logging and Monitoring Policy

7.24 BYOD Policy

1. WeRize doesn't allow BYOD devices to be used for performing WeRize official work purposes.
2. Users are not permitted to use personal devices to connect to WeRize network.
3. If any personal devices to be used for connecting to the WeRize environment have to follow an exception process with approval from the function head/ IT Head.

7.25 Supplier Management Policy

1. Before commencement of any outsourcing arrangement, careful consideration of risks, threats of contractual arrangements and regulatory compliance obligations shall be done.
2. The outsourcing of IT Services should fit into the organization's overall strategic plan and corporate objectives.
3. The terms and conditions governing the contract between WeRize, and the Outsourcing service provider should be carefully defined in written agreements and vetted by WeRize's legal counsel on their legal effect and enforceability.
4. The contractual agreement shall have the following provisions:

a. **Monitoring and Oversight:**
Provide for continuous monitoring and assessment by WeRize so that any necessary corrective measure can be taken immediately in-case of any incidents or mishaps. Outsourcing service provider should have adequate systems and procedures in place to ensure protection of data/application outsourced.

b. **Access to books and records / Audit and Inspection**:

i. WeRize should have the ability to access all books, records and information relevant to the outsourced activity available with the service provider. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the WeRize based on approved requests.
ii. WeRize should have the right to conduct audits on the service provider whether by its internal or external auditors, or by external specialists appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for WeRize.
iii. The contractual agreement shall include clauses to allow the Reserve Bank of India or persons authorized by it to access the WeRize's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats.

5. The Board and senior management of WeRize shall be responsible for 'outsourcing operations' and for managing risks inherent in such outsourcing relationships. The Board of Directors of WeRize shall oversee the effectiveness of the due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions. The Board and IT Strategy committee shall have the responsibility to institute an effective governance mechanism and risk management process for all IT outsourced operations.
6. The roles and responsibilities of IT Strategy Committee in respect to outsourced operations shall include:

a. Instituting an appropriate governance mechanism for outsourced processes, comprising of risk-based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end-to-end manner
b. Defining approval authorities for outsourcing depending on nature of risks and materiality of outsourcing
c. Developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements
d. Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangement
e. Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board
f. Periodically reviewing the effectiveness of policies and procedures
g. Communicating significant risks in outsourcing to the Board of WeRize on a periodic basis
h. Ensuring an independent review and audit in accordance with approved policies and procedures
i. Ensuring that contingency plans have been developed and tested adequately
j. To ensure that the business continuity preparedness is not adversely compromised on account of outsourcing and adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis. Refer: Third Party Risk Management Policy

7.26 Clear Desk Clear Screen

1. Computer terminals shall not be left logged on when unattended and shall always be password protected.
2. Computer screens must be angled away from the view of unauthorized persons.
3. The Windows Security Lock shall be set to activate when there is no activity for a short pre-determined period. The Windows Security Lock shall be password protected for reactivation. *Refer: Clear Desk Clear Screen Policy*

8. Exceptions

Any deviations to this policy will be treated as exceptions with documented approval from the Information Security team.

9. Compliance

Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, be subjected to appropriate disciplinary or legal action in accordance with the WeRize Disciplinary policies. Information Security policies, standards, procedures, and guidelines comply with legal, regulatory, and statutory requirements.

10. References

None