INFORMATION AND CYBER SECURITY POLICY

Abbreviations

S. No	Abbreviation/Acronym	Description
1	AMC	Asset Management Company
2	AFA	Additional Factor Authentication
3	CIO	Chief Information Officer
4	CISO	Chief Information Security Officer
5	COO	Chief Operations Officer
6	CRO	Chief Risk Officer
7	CSP	Cloud Service Provider
8	CTO	Chief Technology Officer
9	DLP	Data Leakage Prevention
10	EDR	Endpoint Detection and Response
11	IS	Information Security
12	IT	Information Technology
13	MFA	Multi Factor Authentication
14	MSP	Managed Service Provider
15	PIM/PAM	Privileged Identity/Access Management
16	PT	Penetration Testing
17	SI	System Integrator
18	SIEM	Security Information and Event Management
19	STQC	Standardization Testing and Quality Certification
20	VA	Vulnerability Assessment
21	VPN	Virtual Private Network
22	WAF	Web Application Firewall

Table of Contents

1. PREAMBLE TO THE INFORMATION AND CYBERSECURITY POLICY

1.1 Document Distribution

This document is owned by Chief Information Security Officer and will be distributed to all the staff through email communication and upload on web portal. It shall also be distributed to the third parties associated with 360 ONE WAM by the respective departments, wherever needed.

1.2 Primary recipients

All Employees of 360 ONE Wealth & Asset Management Group, 360 ONE WAM Ltd (holding company, holding a Merchant Banking licence), 360 ONE WAM Wealth Distribution Services Ltd (covering Stock and Commodities Broking, Depository Participant business and Distribution), IIFL Wealth Prime Ltd (NBFC), IIFL Asset Management Ltd (covering Mutual Funds, Portfolio Management Services and Alternative Investment Funds), 360 ONE Wealth Portfolio Managers Ltd (covering PMS and AIF), and 360 ONE Investment Advisory and Trust Services Ltd (covering Trustee Services and Advisory), collectively referred to as "360 ONE WAM Entity".

1.3 Document Confidentiality

This document is confidential and hence would be made available through internal portal.

1.4 Policy Objective

The objective of this Policy is to set the guiding principles for establishing Information Security strategies to achieve Confidentiality, Integrity and Availability of the information and information systems.

These policies and standards represent the minimum requirements for Information Security that all Businesses within 360 ONE WAM Entities must follow and shall be updated from time to time, by incorporating best practices from standards such as ISO 27001.

Information Security is a business risk management issue. When determining the appropriate level of controls to safeguard 360 ONE WAM Entities' Information, the Business, with the assistance of the Information Security Team, must determine the Risk Level, the highest likely level of threat against the information, and ensure that suitable protection mechanisms are in place. The appropriate level of control depends not only on the risk to 360 ONE WAM Entities, but also on the environment in which the information is stored,
processed or transmitted. These policies define the minimum security that is appropriate for securing the IT resources of 360 ONE WAM Entities. If local laws or regulations establish a higher standard than provided in this policy, 360 ONE WAM Entities' businesses must comply with those laws.

1.5 Policy Scope

These policies and standards are applicable to all locations of 360 ONE WAM Entities within India including all IT and IS assets, all IT and IS processes, all business processes supported by IT and IS and all employees of 360 ONE WAM Entities.

1.6 Review and evaluation

This policy shall be reviewed at the time of any major change in the IT environment or at least once every year. This policy shall be reviewed by CISO for any updation and the reviewed document shall be approved by the IT Strategy committee of directors of the Board.

1.7 Policy Statement

360 ONE WAM Entities' vision is "To become the most respected company in the financial services space in India". As we are operating in a competitive market, our ability to achieve our business goals is dependent on our competence to safeguard our information.

The overall objective of an Information and Cyber Security Policy is to protect the Confidentiality, Integrity and Availability of information assets including those pertaining to its employees, facilities, customers, financial, brand and its reputation.

The main objectives of this policy are:

1. To ensure that all of the 360 ONE WAM Entities information assets including data, intellectual property, computer systems, and IT equipment are adequately and consistently protected from damage or loss, and unauthorized use or access.
2. To ensure information and information systems are available to authorized users as per the business needs and information systems are used in an effective manner to promote 360 ONE WAM Entities vision and to meet its business objectives (360 ONE WAM Entities Values, Business strategy, Customer strategy, People strategy).
3. To meet legal or regulatory requirements and contractual security obligations pertaining to information collection, storage, processing, transmittal, and disclosure (as applicable to 360 ONE WAM Entities).
4. To create user awareness on information and Cyber security as part of the day-to-day operations and to ensure that all employees understand their responsibilities for maintaining information security.

The Information Security Steering Group (ISSG) shall have the overall responsibility of implementation & maintenance of this policy, and it shall review this Policy on yearly basis or if any significant changes occur. ISSG shall also review the compliance & implementation status, effectiveness of controls & their implementation, Internal Audit Reports, Incidents, suggestions & feedback from various stakeholders.

Non-compliance or violation of the 360 ONE WAM Entities Information Security policy shall result in disciplinary action and rules prevalent at the time of violation.

1.8 Roles and Responsibilities

1.8.1 IT Strategy Committee

Refer to IT Policy & Standards

1.8.2 Information Security Steering Group (ISSG)

1. The ISSG constitution shall be similar to the IT Steering Committee as covered in the IT policy and the meetings of ISSG and ITSG will be conducted together at same frequency. It constitutes of the following executives.
    i. Chief Technology Officer (CTO)
    ii. Chief Risk Officer (CRO)
    iii. Chief Information Security Officer (CISO)
    iv. Compliance officer
    v. Head, Operations
2. The ISSG committee shall have quarterly meeting to review Cyber Security Policy and enhancement to achieve target goals. This review and observations shall be placed before the COO and Board meetings.
3. The business entities should communicate suspicious activities to CISO and CIO in timely manner.
4. The formed committee including CISO shall review the incidents or cyberattacks to take appropriate action to strengthen the security.
5. The ISSG shall act as a steering committee for information security the overall responsibility of implementing, promoting and maintaining the Information Security of the organization.
6. The ISSG shall review:
    i. Status of actions from previous IT Steering Committee meetings.
    ii. Non-conformities and corrective actions.
    iii. Audit results.
    iv. Fulfilment of information security objectives.

1.8.3 Chief Information Security Officer

1. The CISO shall report to the Chief Operating Officer (COO) and shall have overall responsibility of implementation of information security at 360 ONE WAM Entities.
2. Custodian of this policy.
3. Review of the Information/Cyber Security policies and procedures on an ongoing basis with a minimal periodicity of once in one year, and suggest incremental improvements (if required) to the same.

4. Propose new initiatives in Information security to the ISSG.
5. Co-ordinate Information Security Internal Audits with the Internal Audit Team and responsible for closure of points arising out of the Internal Audits by co-ordinating with the corresponding departments.
6. Review the JD of respective employees, outsourced staff, vendor employees or participants, who have access to IT systems and Networks.
7. Coordinate External Audits from Certifying Bodies for the period required by the company.
8. Notify any exception to this policy to CRO.

1.8.4 Employees, Associates & Audit Team

All employees, vendors, third parties and any other associates of 360 ONE WAM shall abide by the code of conduct related to Information Security, as laid down in this policy and shall fulfil the information security responsibilities assigned to them.

1.9 Critical Information Assets

1. Network security appliances/solutions: Firewalls, WAF, Intrusion Prevention /Detection Systems, ZScaler, Email Gateway
2. File Servers / databases
3. Application servers for Caliber, Quantis, Wealthspectrum, Omnesys, Greeksoft, CLASS, Salesforce CRM, NSDL DPM, CCIL and Hawkeye Platform
4. Information and Cyber Security appliances/solutions: Next Generation Antivirus and Endpoint Detection & Response, Security Operations Centre

2. ACCEPTABLE USAGE POLICY

2.1 Policy Statement

The purpose of this policy is to define best practices for Acceptable Use of Information and IT assets in accordance with the Information Security Policy of 360 ONE WAM Entities.

2.2 Enforcement

Ethical/regulatory concern process should be invoked to decide whether an ethical/security violation has occurred and to decide on appropriate disciplinary actions as per 360 ONE WAM Code of Conduct Policy and Procedure.

2.3 Internet Usage

1. Internet access is provided to users for the performance and fulfilment of job responsibilities.
2. Users will access Internet for business purposes and restrict non-business activities over Internet. Occasional and reasonable personal use of Internet services is permitted, provided that this does not interfere with work performance.
3. Users shall access Internet only through the connectivity medium provided by 360 ONE WAM Entities. If required, any other medium of internet connectivity can be used after approval from HOD and Information Security Team.
4. Connection to the internet offers an opportunity for unauthorized users to view or access 360 ONE WAM Entities information. Therefore, it is important that all connections be secure, controlled, and monitored.
5. All access to Internet shall be authenticated and restricted to business related sites. 360 ONE WAM Entities shall have the right to filter and prohibit access to certain websites at its own discretion.
6. In case of misuse of the Internet access is detected, 360 ONE WAM Entities can terminate the user's Internet account and take disciplinary action.
7. Users should password protect/encrypt all sensitive information transferred over the internet.
8. Users will schedule communications-intensive operations such as large file transfers, video downloads, mass e-mailings and similar activities during off-peak times.
9. Users shall ensure that they do not access websites by clicking on links provide in emails or in untrusted websites.
10. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.
11. 360 ONE WAM Entities reserve the right to monitor and review Internet usage of users to ensure compliance to this policy.

2.4 Configuration and Installation

1. Users shall not change any hardware configuration, settings in operating system or any applications installed on their desktops.

2. If users require any change in hardware (For e.g. attaching a CD-ROM drive or increase system memory) or software settings, they shall contact the Tech Support.
3. Users shall not install any software or applications on their Information system that is not authorized or not essential to 360 ONE WAM Entities business. If the users require additional software, they should contact the Tech Support.
4. Users will not use or connect modems/data card/any other medium of communication not provided by 360 ONE WAM to their PC/laptop/endpoint unless approved by CISO Team.
5. Accessing external networks including Internet, using modems/data card exposes the entire network to several risks. If the user requires access to external networks through modem dial up/data card, he/she will get the approval from work HOD and Information Security Team

2.5 Protection Measures

To prevent the risk of unauthorized access, users will adopt the following measures:

1. Access while PC is unattended for a short duration; user should lock their PC before leaving their seat.
2. Users shall log out from all applications and turn off the PC when leaving PC unattended for extended period of time or/and at the end of the day.
3. In the case of critical application, users shall take care not to leave the application in the middle of a business activity.
4. Users shall not enable sharing of folders in their PC with other users over the network.
5. For sharing data, the files will be kept on the central server and users requiring access should be authenticated. If required, then access should be provided by the asset owner based on role specific/requirement.
6. Confidential data should be kept on protected servers and must not be copied or/and retained on PC.
7. Access to the Servers / Application shall be based upon User and Authorization Management Policy and Procedure.

2.6 Malicious Code Protection

1. User will not disable installed antivirus agent or change its predefined settings.
2. All files received from external sources will be scanned for virus before opening. This includes files in removable media like CDs/USB, Internet downloads, Email or attachments.
3. User will report any anomaly/unforeseen event detected in the system to system administration team.

2.7 Mobile Device Security

1. Mobile computing devices such as Laptops/ Mobiles Phones /Tablets etc. should not be left unattended in public areas such as airports, hotels and meeting rooms.
2. Users will be responsible for the security of their computing devices (laptops, Tablets & smart phones) provided by 360 ONE WAM Entities and will take adequate measures to restrict physical and logical access to same.

3. Laptops/ Mobiles Phones /Tablets etc. shall adequately protected by using appropriate techniques against unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse.
4. Sensitive information should be protected and neutralized by power-on passwords on the devices.
5. Do not follow links sent in email or text messages e.g. URLs sent in unsolicited email or text messages. While the links may appear to be legitimate, they may actually direct you to a malicious web site.
6. Users having dial up facility are recommended to have personal firewall/anti malware installed to prevent unauthorized access to their laptop while connected to Internet.
7. A loss of laptop shall be reported immediately to the HOD and CISO Team. FIR to be logged within 07 days' post incident.

2.8 Password Security

1. Users are responsible for all activities originating from their user accounts.
2. All passwords are to be treated as sensitive, confidential information. If the password needs to be shared under unavoidable circumstances, care shall be taken to change it at the next login by the owner of the password.
3. Users should not keep passwords residing around on the desks or files/folders/ sticky notes on the system screen.
4. The passwords should be selected in such a way that it is difficult to guess or brute force.
5. Users will change their password regularly. While some applications will enforce password change and complexity on users automatically, it may not be feasible to enforce it for all accounts and for all applications.
6. All operating systems will be configured to lock out the accounts after 5 unsuccessful attempts. If the account gets locked out before 5 attempts.
7. User will report to the Tech Support if account is locked out before 5 unsuccessful attempts.

2.9 Email Usage

1. Users e-mail can be terminated or 360 ONE WAM Entities could take appropriate punitive action in case misuse of the e-mail system is discovered.
2. Users will be provided with a fixed amount of storage space in their mailboxes as defined in the email policy or based on their business requirements at the e-mail server.
3. As mails may be deleted if the storage space is exceeded, users are advised to periodically delete or download older mails from their mailbox into their machines and all e-mails stored locally on the user desktop should be protected by password.
4. The email message including all attached files shall be limited to 3MB size for transmission. Any over-size email message may be restricted from transmission by the email server.
5. 360 ONE WAM Entities have the authority to intercept or disclose, or assist in intercepting or disclosing, e-mail communications.
6. Users should promptly report all suspected security vulnerabilities or problems that they notice with the e-mail system to the Tech Support and CISO Team.

7. Confidential or sensitive information shall not be transmitted over email unless it is encrypted, or password protected.
8. Users owning the email account shall be responsible for the content of email originated, replied or forwarded from their account to other users inside or outside 360 ONE WAM Entities.
9. In case such misuse of the e-mail system is detected, 360 ONE WAM Entities can disable the user e-mail account and take other disciplinary action.

2.10 Document and Storage Security

1. All documents containing sensitive information will be marked as “Confidential” both in electronic and print format.
2. Care shall be taken to ensure confidentiality while these documents are transmitted over email, fax or other communication media or during printing and photocopying of documents.
3. All removable media including CDs, USB or tapes will be labelled as “Confidential”.
4. “Confidential” documents and media will not be kept unattended in the user’s work area, near printers or fax machines and will be stored with appropriate physical security.
5. Users are encouraged to adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorized access, loss of and damage to information outside business hours.
6. Un-used documents/papers will be destroyed using a shredder machine. Expired and bad storage media will be destroyed before disposal.
7. Information assets shall be classified as “Confidential”, “Internal” and “Public”.
8. All information assets shall be labelled as per Classification type and shall be marked in the footer of each document.
9. All confidential classified documents shall be password protected.

2.11 Confidentiality Agreement

1. The employee shall not, either during or after his employment with 360 ONE WAM Entities, divulge or utilize any confidential information belonging to 360 ONE WAM Entities. This includes confidential information on 360 ONE WAM Entities Processes.
2. Employees shall not access, copy, divulge to others, delete or destroy any type of information not in his/her scope of work, belonging to other employees or 360 ONE WAM Entities without the consent and signed approval of at least two members of the Information Security Steering Group whereby one of them has to be the CISO.
3. Employees who have been assigned 360 ONE WAM Entities assets e.g. laptops, Tablets, mobile for internal or external use, must comply with the statements of confidentiality mentioned above.
4. Employees will only use the IT assets provided to them by 360 ONE WAM e.g. hand held PCs, laptops to process or record any business information based on approval from HOD and CISO. All personal mobile devices like smart phones and tablets need to be registered through the 360 ONE WAM Entities Mobile device management platform for accessing business information.

5. If on the termination of his employment, the employee is in possession of any originals or copies of the above-mentioned material, he shall deliver the same to 360 ONE WAM Entities without being asked.
6. The only exception is, when consent to retain them has been given to him in writing by 360 ONE WAM Entities. Any such consent shall not in itself relieve the employee from his obligations under this heading.
7. Employees with access to privileged information shall not divulge that information to third party or even to other employees.
8. Failure of any employee to comply with the confidentiality required above shall give 360 ONE WAM Entities the right to take action as deemed appropriate, including legal action.

2.12 Information Transfer and Exchange Security

1. All departments should ensure that an NDA signed before sharing any sensitive information to third party or any vendor.
2. A list of all the documents shared to third party or vendor should be maintained and signed by both the parties.
3. Exchange of sensitive information through email should be secured (e.g. Word/Excel/PDF can be password protected), Zip the document and use password protection.
4. Confidential information exchanged between departments should be sealed and secured.
5. The recipient should ensure that the information is not modified and shall acknowledge the same.
6. All emails are monitored by the corresponding team.

3. END USER DEVICE SECURITY POLICY

3.1 Policy Statement

1. Ensure adequate control over usage of 360 ONE WAM Entities' desktops/laptops/Tablets/Mobiles.
2. Protect 360 ONE WAM Entities' information systems and assets through appropriate controls over usage of external media and software applications.
3. Ensure that the end-user who has been allotted a mobile / desktop / laptop is made aware of his / her responsibility towards 360 ONE WAM Entities' assets.

3.2 Ownership of End User Device

1. Mobile / Desktops / Laptops issued to staff or consultants remain the property of the 360 ONE WAM Entities.
2. When the mobile / desktop / laptop are allocated to the individual, the user officially assumes "custodianship" of the mobile / desktop / laptop.

3.3 Security of End User Device

1. All the users must agree to take FULL responsibility for the security of their mobile / desktop / laptop and the information it contains.
2. Upon allocation of the laptop, the user must complete and sign a "Mobile Laptop Custody Undertaking form".

3.4 Software on End User Device

1. Users must take all reasonable steps to protect against the installation of unlicensed or unauthorized software and malicious software.
2. The use of unlicensed software (software piracy) is illegal, and use of unlicensed software should be prohibited.
3. Executable software must be validated and approved by their manager, after that approval from CISO team should be taken before being installed into the IT environment.
4. Unmanaged installations can compromise the IT operating environment and also constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.
5. Commercial software (including shareware/freeware) must -
    a. Can be approved by respective Head - IT Infra /CIO and CISO for installation on the 360 ONE WAM Entities resources.
    b. Have a valid license for each prospective user.

3.5 Surrender of End User Device and any other asset given by 360 ONE WAM Entities

1. Upon leaving the employment of, or separation from 360 ONE WAM Entities, the user must return the mobile / desktop / laptop and every other returnable asset to their manager or supervisor or Tech Support Team.

3.6 Secure Usage of End User Device

1. Users shall take special care to ensure that business information is not compromised while using mobile computing devices.
2. User shall ensure that mobile computing devices are updated with latest anti-virus signatures.
3. User shall ensure that all unnecessary services on the mobile computing devices shall be disabled and switched off outside the office premises or when not necessary. E.g. Bluetooth, Infra-Red.
4. Mobiles / Laptops are easy targets for attackers and hence users shall not copy any sensitive data on laptops. If there is a requirement to copy sensitive data to the users shall ensure that:
    a. The mobile / laptop are always kept secured while in a public place.
    b. The mobile / laptop shall never be left unattended and unsecured.
5. Users shall ensure that there are no unprotected shares on their Mobiles / Laptops.
6. While travelling by plane, users shall carry Mobile / Laptop as hand baggage and shall secure with cable lock wherever possible. While travelling by other means, the laptop shall be secured by cable lock.
7. The laptop computer shall be shut down / hibernated and powered off while in transit and in public places, when it is not being used. The laptop shall not be put in a standby mode.
8. Phones/Voice devices used for trading business, customer support should be restricted to specific personals through access control.
9. Calls with the customers should be recorded and back up may be taken and stored at an offsite location.

3.7 Secured usage of Tablet

1. Users shall ensure that they DO NOT change the configurations implemented by the Tech Support thereby leaving the device open to possibility of attack or hijack and in-case configuration change is business requirement then an approval is taken from Head - IT Infra/CIO and CISO.

3.8 Retrieval

1. Retrieval of a mobile computing device shall take place under four scenarios:
    a. Resignation.

b. Termination.

c. Transfer.

d. Issue of a new device in lieu of an old one.

3.9 External USB Usage

1. All USB drives and USB hard disks issued to users shall be registered with Admin Support Team and shall be assigned an asset number for tracking.
2. Use of USB storage devices is not allowed in 360 ONE WAM Entities. For any business reason, if the USB storage devices need to be used, the user shall take an approval from the head of the department along with the CISO team.
3. The Head of Department shall verify the need and shall approve post considering the risk to 360 ONE WAM Entities in case the date is exposed.
4. The user using the USB storage device shall take following precaution while copying data to the USB storage device:
    a. The device shall not be used as a backup device.
    b. The data copied to the device shall be deleted post the work is completed (e.g. PowerPoint file copied to USB device for customer presentation can be deleted post the customer meeting).
    c. Avoid copying sensitive data on USB storage device. If there is a business need to do so, ensure the file encrypted if possible or is protected by password protected archive file.
5. Ensure the USB storage device is not shared with anyone.
6. Loss of USB devices should be treated as an incident and shall be handled as per Incident Management Policy and Procedure.
7. By default, USB access shall be allowed to Chairman, CEO, Executive Directors, CIO, COO and list of approved users, if requested. However, undertaking of the security vulnerability shall be taken from these persons.

4. USER AND AUTHORIZATION MANAGEMENT POLICY

4.1 Policy Objective

1. User Management is standardized, and governance controls are implemented over the Registration, Modification and De-registration of users.
2. Access/authorization should be granted to the users as per business requirements and only against approval from the designated authority based on the principle of least privilege .
3. Users are informed about their legitimate accesses and also educated about the consequences of access violations. Reviews are done of the user management process.

4.2 Third Party Applications / Software

1. For usage of any application which is not in the list of approved applications, approval is required from Business Head and CISO Team along with 360 ONE WAM Entities Exception Request Form.
2. Transactions by users need to have maker-checker controls at the application level. Each transaction needs to be made and checked by separate authorized users. Maker and checker functions can co-exist in a single user, but a single user cannot make and authorize a single transaction.

4.3 Termination / Resignation

1. The HR Department shall inform the date of termination of services to the IT/Tech Team and CISO team within 48 hours after the resignation of the employee is accepted or termination of services decision is taken. HR team shall also confirm if the deactivation/removal of access should be immediate or on last working day.
2. The IT Team will disable/deactivate the e-mail Id, domain id and all the application access are disabled. For SSO enabled applications, domain id disablement would discontinue the access.
3. In case the emails of the employee need to be forwarded to another employee, the Head of the Department & CISO team shall authorize the request and the IRA will send it to the Tech Support Team. The request shall also contain the time period for which the forwarding is required (cannot be more than 30 days of Last working day).
4. In case of other applications, the Application Administrators shall delete or deactivate the user ID from the system on the day of termination of service. (In case of generic user IDs used for applications, the user ID needs to be transferred to another owner).

4.4 Transfer of Employees

1. The HR Department shall inform Tech Support about the transfer of the employee.
2. The Tech Support shall check the access to the applications and other IT facilities available to the employee by referring to the Logical Access Register.
3. The Tech Support shall revoke the access to the application based on approval from the new IRA and inform the HR Department.
4. The user registration procedure shall be followed for granting access at the new location for the new job profile.

4.5 Change of Access Rights

1. The users are responsible to notify if there have been any changes in their roles and the type of access required.
2. The user shall fill the change in access rights form/emails/tickets.
3. The HOD of the user shall verify the required access to be discussed.
4. The user registration procedure shall be followed for granting access to change job profiles.
5. Maker checker process has to be put in case of modification of the access rights.

4.6 Access to Third Party and Vendors

1. Access to third parties shall be restricted based on the principle of "need to know" and as per the principle of least privileges required for operations.
2. Third party or vendor requiring access to 360 ONE WAM Entities resources including network resources from their own systems shall connect through VPNs or VDI or 360 ONE WAM issued laptops. Refer Access Management procedure for further details.
3. It shall be ensured that the third parties and vendors have signed non-disclosure agreement/ clause before granting access.
4. On completion/ termination or extension of the contract, the Head of Department shall send a request for revocation of user access rights or extension of period of access respectively to the Head - IT Infra / Head -IS.

4.7 Sharing of User IDs

1. User IDs shall not be shared by the users.
2. In situations where the login credentials need to be shared, suitable audit trails shall be maintained.
3. Critical user IDs which may be required for emergency procedures may be shared with limited number of system admins to support.
4. Exception to above shall have approval from CISO Team.

4.8 VPN Access

1. VPN access shall be given on the request of user with approval from Business Head and CISO Team.
2. VPN ID creation/deletion/extension shall be initiated through Change Management Process.
3. Reconciliation / Re-certification of the VPN IDs shall be conducted on quarterly basis.
4. For detailed procedure refer VPN Access section in IT SOP.

4.9 Privilege Management

1. Access to information and Information Systems including applications, operating systems, database, and networking / security devices should be provided to users only after proper authentication. The allocation and use of privileges should be restricted and controlled.

2. Every administrative / privileged account should have one-to-one relationship with an individual User. Access to any resource of Information System via shared administrative / special privileges user accounts should not have permitted.
3. The access privileges associated with each system product, e.g. operating system, network, database, application and system utilities, and the users to which these privileges need to be allocated should be clearly identified and documented.
4. Privileged user's access rights (administrative & special privilege) for all Information systems should be reviewed at least every 6 months.
5. For all privileged access, all the user activities should be logged and reviewed periodically.

4.10 Multi Factor Authentication (MFA)

1. MFA shall be implemented for users accessing critical systems.
2. MFA shall be implemented for the users that connect using internet/online facility.

Refer User Access Management Policy

5. PASSWORD MANAGEMENT POLICY

5.1 Policy Statement

1. Define and implement adequate authentication controls in the form of good password controls and disciplines.
2. Control logical access using passwords.
3. Protect business data related application systems, operating systems using passwords.

5.2 Password Security

1. The password controls shall be automated using system features and parameters wherever feasible.
2. Password control will be applicable on all operating system, applications, databases and network devices.
   a. The minimum length of the password shall be 8 characters.
   b. Password shall be combination of alphabets, numbers and special characters.
   c. Password history of at least 3 shall be maintained.
   d. Password age should be minimum of 30 days.
3. All admin and Database passwords - 42 calendar days.
4. Domain and other applications - 42 calendar days.

   a. Users shall be forced to change the initial password set by System Administrator on the first successful logon into the system.
   b. User is not allowed to share password.
   c. Exceptions if any to the above Password Policy and Procedure shall be approved by CISO Team and recorded along with valid reasons.
   d. User should lock the workstation and not to leave unattended desk. Screensaver lock should be configured to lock the workstation if no activity performed for 10 minutes. In domain environment, this control should be forced from the domain policies.
   e. Account lockout parameter value shall be set to 5 wrong attempts and the account shall be locked out for 30 mins.

5.3 Password Reset

1. If the user forgets the password, he / she make a request to the Tech Support providing his employee code. Tech Support will raise a ticket in Service Desk Tool.
2. IT Helpdesk shall then forward this request to the UAM Team in case of domain, One Key and @Risk application.
3. In case of servers and databases, it is sent to Server administrator.
4. For IWIN based applications (except One Key and @Risk), password reset option is available for users.

5.4 Password Sharing

1. Password sharing is not allowed as per the policy.

5.5 Application Password Standards

1. Applications should support authentication of individual users, not groups. In case of groups being used for licensing cost reasons, a proper rationale should be documented and approved by CISO.
2. Applications should not store or transmit passwords in clear text or in any easily reversible form.
3. Default user IDs in the application should be disabled.
4. Default vendor passwords shipped with all information systems should be changed as per the 360 ONE WAM Entities password policy.

6. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

6.1 Secure Area Objective

1. To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.

6.2 Physical Security Perimeter

1. Appropriate physical security controls shall be implemented to protect areas that contains sensitive and critical information and information processing facilities such as data centre, server rooms, office area where sensitive physical documents stored or processed to prevent unauthorized physical access, damage, and interference.
2. Physical access to the critical systems should be revoked immediately if the same is no longer required.
3. Periodic audits and mock drills shall be conducted for addressing the issue of physical threats.

6.3 Physical Entry Controls

1. Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

6.4 Securing Offices, Rooms, and Facilities

1. Appropriate physical security controls shall be implemented to secure offices, rooms and facilities that contains sensitive information.

6.5 Working in Secure Areas

1. Physical protection and guidelines for working in secure areas should be designed and applied.

6.6 Protecting against External and Environmental Threats

1. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

6.7 Public Areas, Delivery, and Loading Areas

1. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

6.8 Equipment Security Objective

1. To protect equipment's from physical and environmental threats to prevent loss, damage, theft or compromise of assets and interruption to the Organizations' activities.

6.9 Equipment Siting and Protection

1. Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

6.10 Supporting Utilities

1. Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities such as electricity, water supply, sewage, heating/ventilation, and air conditioning.
2. UPS, Back-up Generator, Air-conditioning supporting equipment shall be adequate and periodically tested/monitored.

6.11 Cabling Security

1. Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

6.12 Equipment Maintenance

1. Equipment should be correctly maintained to ensure its continued availability and integrity.

6.13 Security of Off-Premises/Off-Site Equipment

1. Security should be applied to off-site assets taking into account the different risks (damage, theft or eavesdropping etc.) of working outside the organization's premises.
2. Adequate insurance cover should be in place to protect off-site and in transit equipment, wherever appropriate.

6.14 Secure Disposal or Re-use of Equipment

1. Any sensitive data and licensed software shall be removed or securely overwritten prior to disposal or re-use of equipment containing storage media.
2. Physical Assets including storage media and systems shall be disposed of appropriately using suitable mechanisms such as cleaning, wiping, overwriting, degaussing etc.

6.15 Removal of Asset

1. Critical equipment, sensitive information or software should not be taken off-site without prior authorization.

6.16 Unattended User Equipment

1. Users should ensure that unattended equipment has appropriate protection.

7. CLEAR DESK CLEAR SCREEN POLICY

7.1 Policy Statement

The objective of this policy is to define best practices for maintaining clear desk and clear screen for security of Information.

7.2 Clear Desk Guidelines

1. Paper and media should be stored in safe place when not in use, especially beyond working hours.
2. Confidential information should be locked away (ideally in a fire-resistant safe or cabinet) when not in use.
3. Employees should not leave the documents or removable media that may contain business information, unattended.
4. Confidential information should never be sent to a network printer, fax machine, photocopiers or scanners without an authorized person retrieving it so as to safeguard its confidentiality during and after printing.
5. Confidential information shall not be displayed on your Pin-Board / Desk.
6. Documents when printed in the network printer should be cleared/collected by the user immediately.

7.3 Clear Screen Guidelines

1. All computers should have password protected screen savers activated or equivalent means of control when unattended.
2. If working on sensitive information, and you have a visitor to your desk, lock your screen to prevent the contents being read.
3. All active application sessions should be terminated upon completion of the work.

8. CRYPTOGRAPHIC CONTROL POLICY

8.1 Policy Statement

The objective of this policy describes the use of cryptographic controls to protect the confidentiality, authenticity and/or integrity of the information across 360 ONE WAM Entities. It also describes the use, protection and lifetime of cryptographic keys across 360 ONE WAM Entities.

8.2 Cryptographic Controls

1. The management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected.
2. Digital Signature Certificate authenticates entity's identity electronically. It also provides a high level of security for online transactions by ensuring absolute privacy of the information exchanged using a Digital Signature Certificate. 360 ONE WAM Entities may consider use of Digital signatures to protect the authenticity and integrity of important electronic documents and also for high value fund transfer.
3. Digital Signature Certificate may be considered for to protect the authenticity, integrity of important electronic documents and also for high value fund transfer.
   Ensure robust mechanism is in place to provide high level of security for online transactions by ensuring absolute privacy of the information exchanged.

8.3 Key Management

1. All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.
2. The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services.

9. MALWARE PROTECTION POLICY

9.1 Policy Objective

The objective of this policy is to install and maintain activities related to Malware Security to avoid threats of attacks from malicious software.

9.2 Anti-Virus Architecture

Two-tier architecture should protect the network.

1. First Layer: A centralized management console should be used to administer the Anti-virus agents on all the hosts on the local network in a location.
2. The centralized console should be used to control the policies for the hosts and the anti-virus administrator should lock these policies with a password. The policies should be as per the configuration documents designed for all systems and servers.
3. All anti-virus installations on all systems and Windows servers should be configured from central console to have.
    a. Daily updates for antivirus updates from central console (and distributed update system)
    b. On access scanning for all files accessed by the user.
4. The second layer: All emails to the users are to be scanned for any malicious code. This is done by default by the Microsoft Exchange Online Protection services offered under the MS O365 subscription.
5. The centralized consoles should be configured for automatic virus definition and engine updates from the Internet (as they become available from the vendor). The centralized console on a priority basis should distribute the engine updates and the other updates.
6. The Anti-Virus Administrator should configure alerts on their respective systems to inform them of a virus incident on the systems under their charge.
7. Anti-virus Administrator should be assigned responsibility to check the Anti-virus logs of the central antivirus console servers on a daily basis and report any incidents to the Tech Support in case of desktop / laptop to check and update this machine and in case of server, report the same to Tech Support for necessary action and also to Information Security Team.

9.3 Handling of Virus Infection

1. Server Level
    a. The Anti-Virus Administrator, Network Administrator and application Support Team should immediately isolate the server from rest of the network if it is a non-critical server and may not impact the business.
    b. In case of critical server, the server should be monitored, and antivirus scanning should be started to reduce the risk.
    c. The impact of the malware should be analysed, and Information Security Team should decide on further course of action.
2. All End User Systems level

a. Users should promptly report any virus infections on their systems to the Tech support and CISO Team.
b. If a user notices a probable sign of infection on his / her machines following actions should be taken.
    i. The user should disconnect the network cable.
    ii. The user should call the Tech Support for assistance.
    iii. The user should not reboot the system until the Tech Support person arrives.
    iv. The user should stop all processing and make a note of the symptoms and any messages that appear on the screen. If it is suspected that the message was initiated by opening an attached EMAIL, a note should be made of who sent the EMAIL.
c. Tech Support engineer should check for viruses or other malicious code on the user's system. It should be ensured that the latest updates are applied for anti-virus programs.
d. Procedures for cleaning of infections provided by the anti-virus software vendor must be followed.
e. In case the virus cannot be controlled internally, the Tech Support should inform the Head - IT Infra, CISO and CTO. The external assistance, if required, should be taken after the approval of CTO.

9.4 Log Monitoring

1. Antivirus logs should be enabled.
2. The Anti-Virus Administrator should report any virus infection
3. Tracking new virus attacks in the industry
    a. During a virus outbreak the Anti-Virus Administrator should be responsible for the immediate fixes or patches available from the vendor and obtaining approval for applying them as early as possible to control damage.
    b. Anti-virus Administrator may subscribe to at least one mailing list for updates from a standard vendor and track the virus activities on the Internet and their modus operandi.

10. VULNERABILITY MANAGEMENT POLICY

10.1 Policy Objective

To ensure the protection of applications and systems by performing periodic Vulnerability assessments and Penetration testing for 360 ONE WAM Entities' application landscape and infrastructure components.

10.2 Vulnerability assessment, Penetration Testing and Red Team Exercises

1. Develop a Vulnerability Assessment Plan and a lot sufficient resources carrying out activities in the plan.
2. Schedule for various security testing exercises such as application security testing, vulnerability assessment, penetration testing, etc. shall be created.
3. Conduct vulnerability assessment and penetration testing exercises for all the critical systems and IT infrastructure of 360 ONE WAM Entities at the time launch. Internet facing applications will be tested periodically.
4. Ensure that the vulnerabilities detected are promptly remediated so as to avoid exploitation.
5. Configuration review of the assets shall be performed in accordance to the approved SCD's.
6. Perform attack and penetration assessments on any new or emerging technologies before they are adopted, mainly public facing systems, as well as a risk-based to test existing applications and infrastructure. Such assessments will only be carried out by professionally qualified teams. In case of any new system/platform not going through the VAT/PT test, then the same should be approved by CISO.
7. Updating and patching of software and hardware should be ensured. Use of outdated or obsolete technology should be avoided as far as possible.

Refer Vulnerability Management Policy

11. CYBER SECURITY PREPAREDNESS INDICATORS

11.1 Policy Objective

To develop a set of indicators that provides adequacy of and adherence to cyber resilience framework.

11.2 Cyber Preparedness Indicator

1. Robust Cybersecurity resilience framework should be defined.
2. The awareness among the stakeholders including employees, third party Vendors, may also form a part of this assessment.
3. Key indicators to evaluate the effectiveness of cyber security resilience framework should be defined, implemented and monitored.
4. Results from monitoring and measurement shall be analysed and evaluated for continual improvement.
5. The indicators should be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals.

12. SOCIAL MEDIA POLICY

12.1 Policy Objective

To combat risk and threats related to social media.

12.2 Social Media

1. Employees and Third party vendors should be educated regarding risk related to social media usage.
2. Social Media risks shall be included in risk assessment and a plan to treat it shall be in place.
3. Any contribution to external social media sites or other outside websites for business-related purposes must be approved by appropriate authority. Please refer to the Media and Social Media Policy for further details.
4. Interested parties should be informed about the penalties for leakage or misuse of 360 ONE WAM Entities' name on social media.
5. Prevent the use of social media on 360 ONE WAM Entities' environment and if permitted should be adequately safeguarded through malware, encryption and antivirus protection mechanisms.
6. Employees shall not violate 360 ONE WAM Entities Privacy requirements while using social media.

13. BUSINESS CONTINUITY MANAGEMENT

13.1 Policy Objective

The objectives of this policy with regard to the protection of information system resources against loss or corruption are to:

1. Minimize the threat posed by the potential loss or corruption of electronic information owned by 360 ONE WAM Entities entrusted to it; and
2. Minimize reputation exposure, which may result from the loss or corruption of 360 ONE WAM Entities' electronic information resources.

13.2 Business Continuity Framework

1. Top management shall ensure that business continuity objectives are established and communicated for relevant functions and levels within the organization.
2. A Business continuity framework shall be established and documented for setting business continuity objectives and defining a holistic approach to implement and execute the business continuity plan.
3. The Business continuity framework shall define the scope of the business continuity management system (BCMS), which shall include all external and internal issues, interested parties relevant to BCMS, legal and regulatory requirements and all the organizational factors and links between BCMS, organization's objectives, policies and risk management strategy.
4. Top management shall demonstrate leadership and commitment with respect to the BCMS by
    a. Ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the organization,
    b. Ensuring the integration of the business continuity management system requirements into the organization's business processes,
    c. Ensuring that the resources needed for the business continuity management system are available,
    d. Communicating the importance of effective business continuity management and conforming to the BCMS requirement,
    e. Ensuring that the BCMS achieves its intended outcome(s),
    f. Directing and supporting persons to contribute to the effectiveness of the BCMS,
    g. Promoting continual improvement, and
    h. Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility

13.3 Business Continuity Planning

1. BCP (Business continuity Planning) committee (consisting of CTO, CISO, CRO, business heads) shall be formed as the decision-making body for the business continuity planning, the key role for this body would be to set a directional tone for the Business continuity initiatives within 360 ONE WAM Entities and review and approval of BIA,

RA and other relevant documents. Further, the committee shall be accountable for ensuring implementation of BCMS across the organization.

2. The BCP team will consist of business IT teams and supports functions and will be tasked with conducting the BIA, Risk Assessments, RTO, RPO definition and implementation of BCMS.
3. The BCP team shall conduct a formal Business Impact Analysis (BIA) on a periodic basis at least annually or on change of business operating model.
4. Risk Assessment methodology based on the results of business impact analysis shall be defined for the business continuity management.
5. RTO & RPO shall be defined basis the risk assessment.
6. A risk treatment plan shall be defined and implemented based on the results of the risk assessment activity.
7. The BCP team should evaluate different recovery strategies based on the RTO and RPO for the application.
8. The strategies shall adequately cover: -
    a. Protection of critical business processes and prioritizing critical activities,
    b. Stabilizing, continuing, resuming and recovering prioritized activities and their dependencies and supporting resources
    c. Mitigating, responding to and managing impacts.
9. BCP committee shall commit adequate resources to ensure that selected strategies are designed and implemented may include but not limited to people, facilities, hardware, software and information both in digital and paper format shall be identified and documented.
10. The BCP plan and procedure shall be designed by the BCP team post approval from the BCP committee the same shall be implemented by having a robust plan that involves stakeholders of critical activities and support functions
11. The confidentiality, integrity, availability & authenticity of the information assets shall be maintained at the time of business continuity implementation. The requirements like physical security of BCP location, employee security, access control parameters etc. shall be taken care off while setting up the BCP infrastructure and executing a business continuity plan.
12. The BCP plan shall also have an adequate response structure with clearly defined responsibilities to be undertaken by personal in case of continuity events.
13. The BCP team should decide the schedules and frequencies of conducting the testing program. BCP testing shall be conducted at least once a year by BCP team.
14. The BCP once finalized shall be communicated to the relevant and concerned stakeholders. Concerned stakeholders shall have a detailed training session as aspect of BCP such as: -
    a. Setting up monitoring mechanisms to detect incidents
    b. BCP plan activation
    c. Execution of a crisis communication plan
    d. Situational response activities

15. The organization shall conduct internal audits at planned intervals.

16. BCP team shall conduct the DR drills on a periodic basis (at least annually) to test the effectiveness of the BCP procedure and any gaps noted in the same shall be leveraged to enhance the BCP.
17. Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

13.4 Recovery

When an information security incident is reported or discovered, the CISO and the CRO will be informed about it. If it involves leakage of sensitive data, then the CISO will also report it to the MD & CEO, the Head of Risk Management and the ISSG.

The asset that is affected by the breach or that is down should be isolated and a workaround plan must immediately be drawn up by the CISO in league with the CRO. A root cause analysis will be drawn up for the failure / breach and the corrective action will be identified. It may involve hardening it with further controls or new patches, or switching to a fresh / back-up system until a long-term solution is deployed.

Refer Business Continuity Management Policy

14. LOG MANAGEMENT POLICY

14.1 Policy Objective

1. Audit Trails / Logs capture adequate details such as user ID, Activity of the user, the location Identifier, the Date & Time Stamp and other relevant details to ensure accountability.
2. System Logs should help in analysing the performance and other issues.
3. Audit Trails / Logs are secured through encryption against unauthorized modifications and should be stored for 2 years for future requirements.
4. The time stamping of logs should be done with the network time server (Clock Synchronization)

14.2 Log Management Strategy

1. Audit Trails / Logs should be enabled on the Application and all supporting Infrastructure components like Databases, Operating Systems, Web Sphere, Switches, Routers and Firewalls.
2. The logs should capture details like user Id, Location, activity and date and time to establish accountability. (Will depend on the current system capability and needs to be defined/scoped accordingly).

14.3 Monitoring and Auditing

1. User activities, exceptions, and security events should be logged and monitored.
2. The activities of users with high levels of access (privileged users such as system administrators and system operators) should be logged and independently reviewed on a regular basis.
3. Capacity utilization shall be monitored.

14.4 Log retention

1. Logs have to retained for Incident management and digital forensics.
2. Online logs have to be available for period of not less than 6 months and offline for a period of not less than 1 year.
3. Access logs have to be retained for a period of not less than 2 years.

Refer Log Management Policy

15. WEBSERVER SECURITY POLICY

15.1 Policy Objective

1. The web servers (intranet and internet facing) are configured for security as per the business, applications and security requirements.
2. Various services made available to the users are controlled and are as per the business, application and security requirements.
3. Traffic to and from the web servers is secured as per the business and application requirements.

15.2 Installation of Web Servers

1. Web servers should be installed on a non-system partition / drive.

15.3 Rename / securely configure the default accounts

1. Before moving the web server into production environment, the web server should be checked for any default / built-in user accounts. These accounts are the first target for the attackers.
2. Ensure that these default / built-in users' accounts are renamed to unique and obscure names.

15.4 Disable all unnecessary Services

1. Any Unused and unnecessary services like ftp, telnet, SMTP etc. should be turned off on the host machine.

15.5 Web server root directory

1. Restrict permission on web server root directory only to the Web Server Administrators.

15.6 Removal of default files

1. Remove all default files which are installed on the webserver during installation.

15.7 Error Messages

1. Configure the web server to display appropriate error messages. The default error messages should be customized to hide confidential and unnecessary details to the users.

15.8 Directory Surfing

1. Disable the option for users to surf through the directories from a web browser.

15.9 Inactivity Time Out

1. The web server should be configured for an appropriate time out if the user remains inactive for a certain number of minutes.

15.10 Concurrent connections

1. Configure the web server for a define number of concurrent connections as per the business requirements.

15.11 Latest versions/Patches

1. Ensure that the web server is up to date with latest patches including the SSL if any installed.

15.12 Registry Keys

1. Ensure that registry keys are added/modified/removed as per the hardening guidelines for each type of web server.

15.13 Set protection against DOS attacks

1. Ensure that appropriate limits are set on the bandwidth usage, “connection time out” and “limit number of concurrent connections” to protect against Denial of Service (DOS) attacks.

15.14 SSL Encryption

1. Secure Socket Layer (SSL) encryption is in place, a minimum 256-bit encryption should be used. In case of any exception, it has to be approved by CISO. Data that travels from and to the websites maintained by the Group is in encrypted format.

16. NETWORK SECURITY POLICY

16.1 Policy Objective

1. Only those services which are required for the business operations are enabled.
2. Integrity and availability of the network infrastructure is maintained.
3. The external connections (inward and outward) are controlled as per business requirements.
4. Private/trusted network is adequately protected against the threats from public/un-trusted network.

16.2 Network Infrastructure Security Controls

1. architecture of the network should be documented by the Network Administrator and the same should be approved by the Head-IT Infra and CISO. Any subsequent changes to the network should also be documented and approved.
2. Firewall should be deployed to provide isolation between External (public) network and Internal Network.
3. Deploy Email and Web Content Filtering Software for protection against spam and viruses.
4. Ensure critical activities such as admin/privilege access and remote connection are logged.

16.3 Network Management

1. Network management tools should be deployed for monitoring and initiating proactive response to the network problems.
2. All network devices should be securely hardened by Network Administrator. (Hardening Parameter Link)
3. Network Administrator should ensure the maintenance of an updated list of all the IP Addresses assigned throughout the network. The IP Address schema should be approved by Head - IT Infra, CISO.
4. Network administrator should ensure that HTTP protocol is disabled on all the LAN, VLAN and WAN devices. But if enabled, it should be approved and proper access control should be in place.
5. Ports/service not in use shall be stopped/blocked.

16.4 Configuration Management

1. Network Administrator should maintain inventory details and configuration of LAN, WLAN and WAN equipment's.
2. Any changes in the configuration should be approved by Head - IT Infra.

16.5 Performance Management

1. Head - IT Infra should define and review uptime requirements of 360 ONE WAM Entities network and it should be part of SLA to be signed with various Service Providers.
2. NOC team should monitor the performance of servers.

16.6 Local Area Network (LAN) Management

1. Network administrator should maintain a map of the network ports and the assigned IPs.
2. A procedure define should be followed before a laptop or desktop belonging to 360 ONE WAM Entities is connected to the LAN.

16.7 Wide Area Network (WAN) Management

1. The activities of the Network Service Providers who has privileged access on the Secret or Confidential machines should be monitored.
2. NOC team should ensure that proactive monitoring of WAN links is done for bandwidth utilization and identifying any suspicious traffic.
3. Network team should ensure that all the WAN Devices are remotely manageable and should have an access controlled management console.

16.8 Wireless LAN Access Management

1. Ensure that security features on wireless devices are enabled (as embedded security features are disabled by default).
2. Tech Support team should ensure that Access Points are placed in centralized location within buildings, possibly away from exterior walls to minimize spillage and maximize coverage. Also should be kept away from sources of possible interference e.g. cordless telephones.
3. Network Administrator should do periodic surveys of Wireless LAN by implementing Wireless Monitoring Tools to check for Rogue Access Points.
4. The procedure defined should be followed before a laptop or desktop belonging to 360 ONE WAM Entities/third party is connected to Wireless LAN.

16.9 Firewall Management

1. Head - IT Infra should ensure that Firewall be installed to segregate the Internal network and External Public network.
2. Head - IT Infra should ensure that:
    a. Firewall is configured to filter packets for correct incoming and outgoing addresses.
    b. Only required services and software are enabled/ installed on the Firewall.
    c. Ports that are vulnerable or not required are disabled on the firewall.
    d. The rules are applied according to the provisions in Internet Security Policy.
    e. Firewall rules are reviewed every year to check for any redundant rules.
    f. Reporting and investigation of any incidents will be as mentioned in Incident Management Policy.
    g. Head - IT Infra and CISO should approve changes to the firewall configuration after assessing the reason(s) for change.

16.10 Network Architecture

1. Networks should be designed in conformance with sound disciplines. The network should be designed to:
    a. Be compatible with other networks used by the enterprise
    b. Cope with foreseeable developments in the enterprise's use of IT
    c. The managed switches should be used to isolate portions of LAN needing higher security and to restrict and monitor traffic between the subnets e.g. VLAN for 3rd Parties ancillary applications like HiD, Canteen system & VLAN for Core applications, etc.

16.11 Network Monitoring

1. Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.
2. Intrusion Prevention System (IPS) is implemented.

16.11 Hardening of Systems

1. The Tech Support Team should ensure that only minimum necessary applications and services are installed.
2. The System or Application Administrator should identify the patches required to be applied and apply the same in case of servers and intimate the Tech Support to apply the same on the desktops/laptops.
3. The Tech Support Team should disable all network protocols and services which are not required for the application.
4. The Tech Support Team should harden servers as per the Server Hardening procedure defined and executed by Infrastructure support team.

17. INTERNET SECURITY POLICY

17.1 Policy Objective

1. Adequate security controls over the access / usage of internet through 360 ONE WAM Entities network

are established.

2. Only authorized users are allowed access to the Internet.
3. 360 ONE WAM Entities network is protected against malicious codes like viruses and worms.
4. Access to the internet is logged and monitored.

17.2 Proxy Server Configuration

1. The Proxy Administrator shall ensure that all Internet traffic is routed through a proxy server and no direct Internet access is allowed unless it is authorized by CISO after justification and approval from HOD.
2. The configuration of the proxy server shall be documented by Proxy Administrator and approved by Head - IT Infra.
3. The Proxy Administrator shall ensure that access to the Internet is logged.

17.3 Granting Internet Access

1. The access permissions to the Internet shall be user/group based. Different users / groups shall have different access permissions.
2. The proxy server shall have a rule base defined for users/groups.
3. Exceptions to above must be based on approval from Business Head and CISO.

17.4 Internet Maintenance

1. The Proxy Administrator shall monitor the logs.
2. In case any changes are required in the configuration/ rule base of the Proxy Server, the Proxy Administrator shall get required approval from Head - IT Infra, Business Head and CISO.
3. The Proxy Administrator shall update the configuration document. The updated document shall be approved by the Head - IT Infra.

18. EMAIL SECURITY POLICY

18.1 Policy Objective

The objective of this policy is to provide guidelines, controls and responsibilities for ensuring that 360 ONE WAM Entities email system is not misused and serves as an efficient mode of business communication.

18.2 Email Guidelines

1. 360 ONE WAM Entities email system is provided to Employees for official purpose only.
2. Employees are responsible for their mailbox management and deleting unwanted emails on periodic basis as every email account will have limited storage.
3. Use extreme caution when communicating confidential or sensitive information via email.
4. Avoid sending large attachments as it consumes lot of bandwidth.
5. Demonstrate particular care when using the "Reply" / "Reply to All" command during email correspondence to ensure the resulting message is not delivered to unintended recipients.
6. Unsolicited email, especially with an attachment, may contain a virus or other harmful software. If in doubt, delete the email or contact the sender to check before opening. Do not open any attachments or web links received from unknown sources.

18.3 Prohibited Activities

1. The following activities are deemed prohibited usage of 360 ONE WAM Entities email systems and are strictly prohibited:
    a. Usages of 360 ONE WAM Entities email system for personal use or usage of Employee's personal account for official communication and vice - versa.
    b. Sharing of username and passwords.
    c. Using 360 ONE WAM Entities email address and passwords on internet sites.
    d. Sending obscene, vulgar or offensive text or material, illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading of computer viruses).
    e. Sending mass mail without authorization.
    f. Transmission of emails that are known to contain viruses or other harmful software.
    g. Alterations of source or destination address information.
2. Employee may note that their emails will be tracked/monitored at corporate level and any violations of this policy will be treated like other allegations of wrongdoing at 360 ONE WAM Entities and shall attract disciplinary actions.

19. INCIDENT MANAGEMENT POLICY

19.1 Policy Objective

The objective of this policy is to define activities related to Incident Management and adherence to the same to ensure quick responses.

19.2 Monitoring and detection:

1. All the devices/appliances/applications of the organisation including servers, endpoints, network devices, applications and any other IT resources shall be integrated with the Security Operations Centre – Monitoring solution.
2. Logs of all the above mentioned devices shall be monitored for any anomalies and
3. Incidents shall be raised, if any, post analysis of the logs and corresponding alerts shall be generated.

19.3 Response and Recovery

1. Alerts shall be raised post investigation including forensic and impact analysis to mitigate and prevent incidents.
2. Response and recovery shall be aimed at timely restoration of the systems affected, if any, in line with the Business Continuity policy.

19.4 Incident Types

The incidents should be classified as non IT incidents (e.g. unauthorized access to confidential information, loss of theft of Mobile, laptop or IT equipment etc.) and IT incidents (e.g. DDOS, Email spoofing etc.)

19.5 Incident Reporting / Logging

1. All IT incidents should be logged in Tool by tech Support.
2. All Non- IT Incidents should be informed to Admin/HOD, Tech Support Team.
3. IT Incidents should be classified as per Service Catalogue as discussed with Service provider and signed off by CISO/Head IT Infra.

19.6 During Working Hours

1. Reporting shall be done through appropriate management channels as quickly as possible.
2. Tech Support shall decide the severity level of the IT incident and shall inform Head IT Infra and CISO Team and Logged call in Kaseya
3. Information related breaches:

    i. All level 1 incidents shall be immediately reported to the Head IT Infra and CISO Team

    ii. The time to take corrective action shall be as follows:

    - 1st Level: Immediately or at the earliest by Head IT Infra and CISO Team.

- 2nd Level: 8 hours failing which the IRA's shall escalate the matter to relevant Head IT Infra, CTO and CISO Team.
- 3rd Level: 24 hours failing which the ISR/Head of Department shall escalate the matter to relevant COO/Senior Management

19.7 During Non-Working Hours/ Holidays:

1. For incidents that happen after normal working hours, following sequential actions shall be followed:

    i. The concerned employee shall focus on containing the damage and dealing with the crisis using all available assistance.

    ii. The concerned authority shall be reached to inform on the incidents within a reasonable time and as early as possible.

    iii. The reporting procedure shall remain the same.

19.8 Recovery and restoration

1. The primary focus is to contain the incident once it's verified and to prevent the incident from horizontal or vertical movement.
2. Logs shall be investigated and the concerned shall be notified of all the actions.
3. Recovery from backup or shifting to secondary/DR site shall be carried out, if necessary to ensure Business Continuity.

19.9 Analysis of the Incident

1. The respective teams shall collect evidences and audit trails of all the incidents from the relevant personnel.
2. If the incident cannot be resolved by known means, then root cause analysis shall be carried out by the concerned departments.
3. Based on the analysis appropriate workarounds, preventive or corrective controls shall be suggested.
4. The root cause analysis and the action taken report shall be submitted to the CISO Team for approval.

19.10 Sharing Incidents with other locations

The incident records and metrics shall be coordinated by the Incident Manager centrally for all locations and he/she shall, where relevant and useful, provide the incident related information to other locations to benefit from preventive or corrective actions taken.

19.11 Management Reporting of the Incident

1. The IRA shall compile a report of all non-IT incidents if any and forward it to CISO monthly basis.
2. A copy of the report shall also be sent to the Head HR for taking disciplinary actions, if required.
3. All unusual information security incidents should be reported to the Reserve Bank of India, DNBS Central Office in Mumbai as specified in Point No. 2 of Annex I to the RBI Master Direction for NBFCs using the template provided in Annex I.

4. For Incident and Cyber Crisis, a comprehensive management plan shall develop and maintained.
5. All information security incidents involving cybercrime and network attacks should be recorded, assessed, and reported to the regulatory and nodal agencies such as CERT-IN.
6. An effective Incident Response strategy shall be in place to deal with post incident damage handling which if not discovered or detected by the organization, in the first place can lead to serious damage to the organization. Incidents can be physical, environmental or computer attack related.
7. All types of unusual security incidents as specified in point No. 2 of Annex I which deals with Basic Information including Cyber Security Incidents as specified in CSIR Form of Annex I (both the successful as well as the attempted incidents which did not fructify) to the DNBS Central Office, Mumbai. The other particulars of the reporting have been provided in template as per Annex I.

19.12 Remote working and Teleworking

As per the Business Continuity policy, staff and critical third party resources may work from secondary location to ensure Business continuity in case of an incident or emergency. In case of an incident resulting in not able to reach the office premises, staff may carry out their operations from the chosen secondary location through secure VPN. This is applicable to the following.

a) Natural disasters – Floods, earthquakes, fires etc.
b) Man made events – curfews etc.
c) Pandemic and hazards – Outbreak of Covid etc.

Refer Cyber Security Incident Handling Policy

20. IS AUDIT POLICY

20.1 Policy Objective

The objective of this policy is to define activities related to Information System Audit and adherence to the same to ensure RBI Framework.

20.2 IS Internal Audits

1. The audits should be performed as per the 'IS Audit Plan'.
2. 360 ONE WAM Entities to adopt IS Audit framework duly approved by the COO/Board.
3. IS Audit should be conducted at least once in a year and outcome of the IS Audit to be reported to the Audit committee.

20.3 IS Audits

1. IS Audits should be performed by qualified systems auditors with good knowledge / experience in this area.
2. 360 ONE WAM Entities to have adequately skilled personnel in Audit committee who can understand the results of IS Audit.
3. The main objective of the IS audit is to review the configuration of technical areas like Applications, Databases, Web Servers, Operating Systems, Network infrastructure. etc.
4. Systems should be audited on an annual basis by an independent CISA / CISM qualified or CERT-IN empanelled auditor to check compliance. Organization shall submit the report to SEBI along with the comments of the Board of AMCs and Trustees within three months of the end of the financial year.
5. Depending upon the availability of skilled resources Systems Audits should be performed by Internal Teams or could be partially / completely outsourced. This audit should be conducted at least a year
6. IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up.
7. While designing the IS framework, 360 ONE WAM Entities shall leverage the guidance issued by Professional bodies such as ISACA, IIA, ICAI in this regard. ICAI has published "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" on the subject.
8. 360 ONE WAM Entities shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit.
9. 360 ONE WAM Entities management shall be responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance should be clearly delineated in the framework. The framework may provide for an audit-mode access for auditors/ inspecting/ regulatory authorities.

20.4 Vulnerability Assessment and Penetration Testing (VA-PT)

1. This is a highly technical area and calls for usage of specialized tools, techniques and skills.
2. While performing VA-PT of any information asset, care should be taken to ensure that:
    a. An authority letter is given to the external users/firm OR internal users to perform VA-PT
    b. The administrator is put on alert.
    c. VA-PT closure should be tracked.

20.5 IS Audit Plan

1. A detailed IS audit plan shall be prepared to ensure that all critical information assets are covered with the above described three stage approach.
2. The IS audit calendar should be planned and scheduled in such a way that the audits should not become hindrance to the day-to-day operations of the business.
3. The auditor and auditee should be given adequate notice about the audit.

20.6 Audit Reporting

1. ISMS Audit Reports giving details of the findings should be submitted to the designated user for rectification (correction) and improvement in the controls (corrective action).

20.7 Classification of Findings

1. The findings of IS Audits should be classified.

20.8 Corrective Action

1. The observations raised in the IS Audits should be studied, classified based on their severity and taken up for rectifications. This study also involves a systematic investigation of the “ROOT CAUSE” of identified problems or identified risks, with an objective to correct them (correction) and improve the control (corrective action).
2. The Auditee should prepare a report mentioning target dates of correction/corrective action (where immediate correction / corrective action is not immediately possible) for the audit findings. Thereafter, these reports should be submitted to the Information Security Steering Group (ISSG) for review and further actions (if required).

21. SEBI UPDATES

1. In case of critical activities that have been outsourced to different agencies / vendors / service providers, an appropriate monitoring mechanism should be clearly defined to ensure that all the above requirements are complied with. The periodic report submitted to SEBI should highlight the critical activities handled by the agencies and certify that the above requirements are complied.
2. Quarterly updates and reporting to SEBI about Cyber-attacks and threats and measures taken to mitigate vulnerabilities, threats and attacks by Compliance team.

22. TRAINING AND AWARENESS

1. This policy will be shared with all employees. Awareness about this policy and the importance of information and cyber security will be imparted at the time of induction, and this will be embellished with periodic training / reminders on Information Security by the Technology and HR teams.
2. Information/Cyber Security awareness shall be imparted to the employees and outsourced staff including consultants, contract employees etc. periodically through classroom/virtual classroom/Learning Management/emailers/Phishing campaigns etc.

23. THIRD PARTY INFORMATION SECURITY RISK MANAGEMENT

23.1 Objective

Third party products and services are utilized during the course of Business. Third party relationships carry risks that must be addressed as part of due care and due diligence. Objective of this policy is to put forth the requirements on how the Third party risk management is carried out.

23.2 Scope

This policy is applicable to all the Third party relationships that the organisation engages in to procure products or services to carry out its business operations.

23.3 Definitions

Employee: A person who is hired to work part-time or full-time for the organisation and not an independent contractor.

Third party or 3rd party: Any person or organisation who provides a service or product (to organisation) and not part of the organisation.

23.4 Policy

1. All Third parties granted access to organisation's Information resources must sign Non Disclosure Agreement and any other applicable agreement as per the engagement.
2. All Third party relationships must be evaluated for Information Security Risk prior to any interaction and must re evaluated at least once annually or any time there is a change to the organisation.
3. Third party relationships with significant Risk shall be provided with recommendations to lower their exposure or any other action based on the Business requirement. These relationships will be re-evaluated to arrive at the residual risk post implementation of the recommendations.
4. Third party relationships pertaining to critical products or services to the organisation or multiple products or services to the organisation shall be assessed more thoroughly.

24. CLOUD SECURITY

24.1 Objective

The purpose of this policy is to define the security for cloud-based activities that support the organisation's information systems, networks, data, databases, and other information assets.

24.2 Scope

The scope of this policy is for all information technology systems, software, databases, applications, and network resources that are implemented in cloud-based and/or managed service infrastructures needed by the organization to conduct its business.

24.3 Policy

1. All the policies viz Data Security, Access management, password policy etc. pertaining to the organization shall apply to the cloud based products and services also.
2. Cloud services shall be taken only from Ministry of Electronics and Information technology (MeitY) empaneled Cloud Service Provider (CSP) and the CSP's data center shall hold a valid Standardization Testing and Quality certification- STQC (or any other equivalent agency appointed by the Government of India).
3. In case of SaaS and PaaS engagements, the underlying infrastructure/platform shall be from MeitY empaneled CSPs only.
4. A back-to-back agreement, clear and enforceable agreement shall be in place with the CSP, and System Integrator (SI) or Managed Service Provider (MSP), if any, with an explicit and unambiguous delineation of responsibilities for all activities.
5. Use of clouds services must comply with the law of the land and regulatory guidelines for the organization.
6. All the cloud based products/services shall be configured properly and ensured that data is not getting leaked.
7. Risk assessment of the internal and external threats and vulnerabilities, as applicable to all cloud environments has to be conducted prior to engaging.
8. Development, testing, staging, production etc. environments shall be properly configured and ensured that the production environment is segregated from the other environments.
9. Obsolete or old environments that are not in use have to be decommissioned and data has to be properly disposed off, if any.
10. All the services/applications/infrastructure on cloud shall be integrated with Security Operations Center (SOC) for continuous monitoring and incident management.
11. Data at rest or in motion, within any approved cloud environment, must be protected as per the Data Security policy.
12. Anti Malware solution shall be implemented, wherever applicable.
13. Availability for the cloud based applications and services has to ensured in line with the Business Continuity policy.

14. Incident Management shall be practiced for the Cloud based products and services as per the Incident Management policy.
15. Appropriate service level agreements (SLAs) with cloud service providers are to be put in place to ensure acceptable third-party cloud vendor performance.

25. REMOTE ACCESS MANAGEMENT

25.1 Objective

The objective of this Policy is to set the guiding principles for establishing remote access management to achieve Confidentiality, Integrity and Availability of the information and information systems.

25.2 Scope

The scope of this policy is for all personnel, information technology systems, software, databases, applications, and network resources needed by the organization to conduct its business.

25.3 Policy

1. Access to 360 ONE WAM resources such as applications, infrastructure, development environment etc. remotely shall be provided only through 360 ONE WAM provided laptops/desktops/any other devices or VDIs provided by 360 ONE WAM or through the whitelisted VPN of the respective organization only.
2. Devices such as mobile and tablets are not permitted to carryout teleworking. Access to production environment/data shall be through VPN in concurrence with PIM/PAM solution or through VDOIs only.
3. Access shall be provided as per the access management policy after necessary approvals and all access provided shall be reviewed quarterly.
4. Remote access through VPN shall be provided on official devices identified/provided by 360 ONE WAM vide agents installed on the devices. These devices shall be configured with necessary solution stack and necessary security measures shall be implemented to ensure that the security configuration of these is not tampered with.
5. Multi factor Authentication (MFA) shall be implemented for remote access. Access to resources from Mobile devices shall be through Mobile Device Management (MDM) only with restriction to ensure data leakage prevention.
6. Data in transit and data at rest should be encrypted with strong encryption. Customer data shall not to be shared with vendors in any format in any manner apart from the access mechanisms specified in this document.
7. All the applications/VDIs/VPN/MDM shall be integrated with SOC (SIEM) solution and they shall be continuously monitored by SOC (SIEM) Team.
8. Any incident observed must be reported to CISO team for investigation without delay. Any exception to the policy shall be approved by both CTO and CISO.
9. In case of BYOD devices classified as official devices, the applicable list of applications shall be as per the organisation policy and Business requirements. These devices shall be subjected to periodic audit.