NAVACHETANA

IT POLICY

SHAISHAVI PROJECT CONSULTANTS

TABLE OF CONTENT

IT POLICY

1. INTRODUCTION

The IT policy of Navachetana is devised with intent to serve as an IT infrastructure usage guide. The operating procedures listed in the IT policy document ensures that the returns from IT infrastructure are maximized while minimizing any negative impact of policy violation.

The document also lists the key process owners, basic IT processes, outline of steps to follow, do's and don'ts, escalation procedure & issue resolutions.

Security policy is also an integral part of the IT policy. The security policy is a preventive mechanism for protecting important organization data. It communicates a coherent security standard to users, management and technical staff. It analyzes the threat, vulnerabilities and potential risks, thereby establishing control objectives and recommends controls.

2. GENERAL

The technology and infrastructure required for employees is provided by Navachetana. The organization takes the responsibility of maintaining the infrastructure, securing it against unauthorized access and informing users of the expected standards of conduct including responsibility for reporting violations.

Attempts to violate policies are regarded as a breach in the code of conduct and can result in a disciplinary action against the employee.

The organization shall also adhere totally to the local laws and use of IT infrastructure to break the law will be regarded as a 'criminal offence' and reported to the concerned authorities.

Privacy & Ownership

All IT equipment and infrastructure used by the employees within the organization is considered property of the Navachetana. The programs created as well as any data that resides on the desktops and laptops allotted to the employee are also the property of Navachetana.

The organization reserves all rights to monitor and review all data on the employee's computer hard drive. The computer allotted to an employee is for the specific duration of his employment within the organization. The employee may be allotted a desktop or a laptop based on the role that he/she performs within the organization.

Once a computer is allotted, the employee should not swap or change the allotted machine with others. In cases where there is such a requirement, the employee should raise the request to IT helpdesk. The employee shall be fully responsible for any material found on his / her computer's hard disk.

Software Licensing

All operating systems and software used in the organization shall be licensed to Navachetana. Employees are prohibited from downloading and using unlicensed software or using license keys from external sources.

Any shareware – freeware that is required by the employee or is evaluated by the employee and loaded should be discussed with his / her line manager. In the event of this being evaluated as a useful program, the same shall be intimated to IT helpdesk and standardized. The tools and editors used by the employees shall also be as per the IT standards.

Usage of Mail & Internet

Each employee shall be provided with an e-mail ID that is in the Navachetana domain. The employees are expected to manage their passwords responsibly as well as use the mail facility regularly to respond within a reasonable amount of time. The facility shall be used by and large for official communications meant for Navachetana business. The organization however recognizes the need to exchange personal communications occasionally. These messages should not be large enough to block the network.

The content of messages should not be offensive or involve any unlawful activity. The content should not pertain to:

- Discrimination on basis of race, creed, colour, nationality, religion or political beliefs
- Harassment - sexual or otherwise
- Copyright infringement
- Personal business interest

Employees are required to maintain password confidentiality to avoid unauthorized usage. Forwarding of chain mails and sending mail to ALL should be avoided as far as possible.

Internet usage for official purposes is encouraged. No explicit permission is required to get access to the internet and it is assumed that the employees will use this facility with discretion. Appropriate uses of internet include:

- Communication with other agencies or business partners,
- Discussions for professional development
- Information on industry trends
- Research of policies – technical issues
- Timely access to publications related to work
- Advancing information need of the organization

Inappropriate usage of internet can result in disciplinary action against the employee. This can range from verbal warnings to termination of employment based on the severity of conduct. Inappropriate usage would include:

- Unauthorized attempts to break into any computer whether of Navachetana or another organization (Hacking)
- Using working time, equipment and/or other resources for non-work-related activity, personal gain or recreation
- Sending threatening messages
- Sending racially and/or sexually harassing messages
- Theft, or copying, of electronic files without permission
- Sending or posting confidential materials outside Navachetana to non-authorized personnel,
- Sending chain letters through electronic mail
- "surfing" pornographic and sexually oriented sites

Confidentiality

All information on the computer systems including the programs and data (whether customer or test data or documents) is considered confidential. These should not be shared with external parties without specific consent of the Manager.

Programs and data are also available on shared repositories and servers. This data is also confidential and for the purpose of sharing within the organization. Removal of this data is prohibited.

Passwords Sharing

Passwords to specific resources (servers / databases) are provided on a need basis. This needs to be maintained confidentially and should not be shared with other co-workers and employees.

Obtaining passwords to resources should be sanctioned by the line manager before the IT department processes the request.

When the employee moves out of the specific role and does not require access to the resource, he / she / his line manager needs to make sure that the access is revoked.

Shared Files Usage

Employees are required to share only those required folders to prevent / discourage unauthorized access to the data on their computers.

As a corollary, employees should not delete, read, copy or modify files of other users and /or data belonging to others without their consent.

Usage of External Media

Usage of external media should be restricted and only on a need basis. Media request has to be authorized by the manager and submitted to the IT helpdesk who would procure the media. Typical reasons for requesting media includes back up of data, sending files / programs to data centre etc.

USB memory carried by employees will need to be scanned for viruses. Employees are prohibited from copying copyrighted source code and other material from the network on to media without prior permission.

It shall be the responsibility of the employee to make sure that the media does not have any virus or malware.

Personal Usage

Employees of the organization will be required to use the software programs and the operating systems installed on the computer. In the event of a new software requirement, such a request should be routed to the IT helpdesk.

The list of authorized and licensed software loaded on the employee's computer is for usage for office purposes. This software should not be removed from the machine. Nor should the employee use the license keys and load the software for personal use in different machines outside or inside the office premises.

Employees are also required to not load media, games, screen savers and any other questionable material on the computers allotted to them.

3. INFORMATION SECURITY

Security Layers

Physical Security

Physical security is the action taken to ensure that the computer system components (CPU, monitor, keyboard, printer etc) are secure and not accessed by unauthorized personnel. Physical security is implemented by means of restricting entry of unauthorized people into the working areas of the organization. The Administration department takes on the responsibility of implementing physical security.

Any third-party personnel entering the organization for maintenance of the computer systems will need to login the details at the Security and shall be guided to the IT helpdesk.

Access Security

Access security is implemented through the use of passwords for shared areas and network administration.

The various servers are secured with passwords. Based on the server function, an authorized person from the corresponding department takes on the ownership of maintenance of the server. He / she will work closely with the IT helpdesk.

Information Security Education & Training

All employees of the organization and, where relevant, third-party users shall receive appropriate training and regular updates in organizational policies and procedures. E.g. log-on procedure, use of software packages, before access to information or services is granted.

Response to Security Incidents & Malfunctions

Employees should report security incidents through appropriate channels as quickly as possible. This can be any suspected hacking or access of their computers, wrongful usage of their e-mail or even observed actions of colleagues that are a potential risk. These incidents are to be reported to the IT helpdesk.

In case of any other malfunction of an installed program or the computer hardware, the overall procedure would be as below:

- The symptoms of the problem and any messages appearing on the screen should be noted.
- In case of virus attacks, the computer should be isolated and use of it should be stopped. The IT helpdesk should be alerted immediately.
- Users should not attempt to remove suspected software unless authorized to do so.
- Appropriately trained and experienced staff should carry out recovery.

Security Governance

Information security forum to review, agree and promote information security activities within the organization. The forum shall be convened by the IT owner within the organization along with the IT helpdesk.

This forum shall undertake the following activities on a periodic basis:

- Review and approve information security policy and overall responsibilities;
- Monitor significant changes in the exposure of information assets to major threats;
- Review and monitor information security incidents;
- Approve major initiatives to enhance information security.

4. ACCESS CONTROL & USER MANAGEMENT POLICY

The purpose of the policy is to secure information assets, employees and information processing facilities of Navachetana by defining rules for the creation, monitoring, control and removal of user access to IT assets and services based on the business requirements.

This document sets out Navachetana arrangements for limiting the access to information and information

processing facilities based on ‘need to know –need to do’ principle; ensuring authorised user access and to prevent unauthorised access to systems and services; making users accountable for safeguarding their authentication information; and preventing unauthorised access to systems and applications.

User Access Provisioning

- Navachetana shall establish and implement an authorization process for all user access privileges to all systems based on job roles and nature of information handled by them. All such privilege determination process shall be documented, approved and periodically reviewed.
- Passwords are currently the principal means of secret authentication of a user and validating their identity to access to the Information Systems and services.
- Systems and applications that contain sensitive or confidential information shall be segregated; isolated and appropriate access controls shall be made available to prevent data leakage.
- Revision of access privilege shall take place whenever there is a change in the organizational status of employees, including termination or transfer of users.
- The allocation of user access privileges to information systems and services is controlled as contained in this policy and any management directive that may be issued in this regard.
- This policy is supported by a set of formal procedures that are in place, covering all stages in the life-cycle of user access management; starting with initial registration of new users and ending with the final de-registration of users who no longer require access to information systems and services. User shall be given access to the systems / devices using an individual username and password. Username and password used by the users shall follow the (Password Management Policy).
- At least once in six months, NAVACHETANA shall review the user access that has been granted and ensure that access privilege granted is still valid.

- On the request of the Business Unit Head or top management, access privilege shall be temporarily suspended, modified or disconnected from the network if it appears that any applicable company policy has been violated or that a user's activity is or could be a threat to the secure operation of Navachetana networked information system.
- In order to ensure accountability of usage, access to IT resources shall be through individual user accounts. Users are responsible for security of their system and shall take adequate measures as mentioned in (Acceptable Usage Policy) to prevent unauthorized access to their system.
- To protect the confidentiality of data, session time out shall be enabled with the help of password protected screen savers.

Network Access Control

- All network and systems devices shall be identified on the network to enable the administrator to implement controls and to ensure accountability. Access to network devices and network services shall be based on job requirements. Appropriate security measures shall be adopted to prevent unauthorized access to NAVACHETANA network from outside.
- Sharing of folders and files within the network shall be controlled. Access to files and folders shall be given based on 'need-to-know' and 'need-to-do' basis. Users shall be authenticated over the network using unique username and password to ensure accountability.
- Access to network devices shall be through secured means and clear text protocols shall not be used. Unnecessary services shall be disabled.
- Appropriate segregation of networks shall be enforced using the concepts such as DMZ (Demilitarized Zone) and VLAN (Virtual Local Area Network). External connection to the network shall be protected with the help of gateway firewall and proxies. All network devices shall have appropriate connection time out and shall display suitable warning banners to provide legal protection. Proper authentication mechanism using username and password shall be used while connecting users from external network to the NAVACHETANA network and through secure means such as VPN.

Administrative Access Control

- The administrative access to servers, applications and network devices shall be restricted to only required number of administrators. Usage of common user IDs, default user IDs and password is strictly prohibited and adequate logging and monitoring of administrative activities shall be enabled. System documents such as network diagrams, process flow-chart are to be maintained securely and hard copies are to be kept in lock and key.

- Review of access to administrators shall be done at least once in six months to assess if high privilege access is still required for business purpose.
- Access to configuration ports of network devices shall be protected from unauthorized usage. Unused configuration ports shall be manually shut down. All configuration ports shall be password protected. Default user names and passwords that may exist on the network device shall be removed.
- System and network administrators shall use system utilities to carry out certain functions as part of their day-to-day operations. Appropriate controls need to be established to protect access to system utilities.

Third Party Access Control

- External parties (including suppliers, vendors, visitors and contractors) are prohibited to access the IT infrastructure without Navachetana approval. Access shall be based on business requirement and on the principle of minimum required privileges. Approval for access shall be sought from the Sr. Manager (IT) and the following information shall be clearly stated: system, services to be accessed, duration, purpose and country. Approval is not required for demo systems that reside outside the Navachetana LAN or demo systems residing within Navachetana DMZ.
- Prior to providing access, the external party shall sign a non-disclosure agreement (NDA) with Navachetana addressing information security risks associated with information and technology services
- Visitors shall not be allowed to utilize any equipment or systems unless authorized by the Sr. Manager (IT) and the owner of the system. Access to systems shall be granted only on written confirmation by the owner of the system. The confirmation should include the application system, functions to access, permitted rights and the duration. Systems of the external parties shall be connected to the network only after it is ensured that the system is secure by way of appropriate agreement/audit. If the workstation connecting to NAVACHETANA infrastructure is owned by the visitor, it should have up-to-date anti-malware software installed and running. The workstation must not be connected to Navachetana network and any other network at the same time. When the stipulated time period ends, the approver should be notified and access to the systems should be revoked.
- When access is given to external parties, their activities shall be appropriately controlled and monitored. The external parties shall be briefed on the security policies of Navachetana.

5. INFORMATION & ASSET CLASSIFICATION

Inventory of Assets

Navachetana shall ensure that an appropriate inventory is maintained for all the IT assets. Assets shall be identified with the help of unique tags which includes all relevant details about the assets. An owner shall be identified for each asset. Apart from the inventory that is maintained for IT assets, an information inventory shall be maintained which will list down critical information that is maintained by Navachetana.

Users in Navachetana shall ensure that information and information assets are used for business purposes and as per Acceptable Usage Policy. All users including contractors and third-party users, at the time of their separation, shall return all assets in possession of them acquired through the duration of engagement with Navachetana.

Information Classification

Information created by users is the exclusive property of Navachetana. Based on the criticality; information shall be classified and labeled. Information classification shall be reviewed annually. In order to prevent unauthorized disclosure or misuse, suitable procedures for handling and storing classified information shall be established.

All information shall be classified according to its sensitivity and confidentiality. The asset (data) owner shall appropriately classify the information according to the following guidelines.

- **Restricted/Sensitive**: Information that is extremely sensitive and intended for use only by named individuals within the organization. Restricted information may not be shared with external parties unless it is in compliance with legal requirements or there is a strong business justification.
- **Confidential**: Information that is sensitive within the organization and is intended for use only by specified groups of employees. Such information shall be shared within a specific department and access by personnel of other departments is restricted.

- **Internal**: Non-sensitive information available for usage within NAVACHETANA. Information classified as internal is not suitable for release outside the organization.
- **Public**: Non-sensitive information available on public domain that can be accessed by anyone.

When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources. If any information is not specifically classified it shall be treated as ‘Internal” by default.

Based on the classification of the assets, the information shall be labeled. The labeling must be made available on the documents and in a visible format. Detailed procedure for protecting different classification of information is given in Asset Management Procedures.

6. ANTI VIRUS

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. A malware is an abbreviated term meaning “Malicious Software”. Both are together termed as “virus” in this policy document.

Viruses can be transmitted via e-mail or attachments, downloaded Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to NAVACHETANA in terms of lost data, staff productivity, and/or reputation. Therefore, one of the goals of NAVACHETANA is to provide a virus free computing network.

Antivirus Application

- IT Department shall ensure that any workstation (servers, desktops and laptops) that is connected to the network is installed with the company approved antivirus program.
- A new system shall be allowed to connect to the network only after it is verified that it has adequate virus protection mechanism.
- Antivirus agents that are installed on the client systems shall be password protected to ensure that end users cannot uninstall the agent. Similarly, the end users shall not have any privileges to change any configurations or disable the agent.

- While upgrading the systems (migrating to new operating system), it should be ensured that the antivirus agent can support the new system and provide adequate protection.
- Adequate number of licenses to cover all systems shall be available for the antivirus application.

Antivirus Scan

- There shall be a regular scan of all the systems. All the systems including the applicable servers shall be scanned once a week and a detailed report shall be reviewed by the IT Department. Users are prohibited to disrupt or disable scanning of their system.
- Any system that is not turned on during the scheduled scanning time will be scanned for virus immediately when it is turned on.
- All files that are downloaded from internet shall be automatically scanned for virus infections and shall be either quarantined or deleted as appropriate. Similarly, any files copied from removable media (CDs / USBs) shall also be scanned appropriately.
- Any attachment that is received or downloaded shall be appropriately scanned by the antivirus application.

Tracking New Outbreaks & Antivirus Updates

- IT department shall regularly monitor for any massive outbreaks and take adequate measures such as downloading specific tools or carrying out manual procedures to clean virus infections.
- Virus signatures are to be updated on a regular basis.
- Adequate redundancy mechanism shall be made available to ensure that virus signatures are available if the main sources for providing antivirus updates are not available.

7. BACKUP & RESTORATION

Frequency & Scheduling

- The frequency for taking a backup shall be determined by the business unit head in consultation with the IT Department. Backup methodology has to be selected as appropriate among full backup, incremental backup and differential backup types.

- The backup process shall be scheduled in such a way that it does not affect the business operations. Backup shall be scheduled before and after the execution of critical points in time such as end of day, end of month, end of year. Wherever it is possible backup tasks shall be automated.
- Selection of backup media shall take into considerations the data that is going to be stored and other factors such as shelf life, rotation etc. Ease of usage shall also be considered before the selection of the media for backup.
- Whenever there is a change in the system environment, such as application, operating system etc., it should be ensured that the backup information retained shall be compatible with the new system environment.

Security & Restoration

- The backup information is as critical as the original information. Adequate security controls (both logical as well as physical) shall be enforced to ensure limited access to backup data.
- Backup media shall be stored in a fire proof cabinet under lock and key.
- Backup media shall be stored in an offsite location to prevent the destruction of both the main source and the backup source.
- On a periodic basis backup shall be restored and tested for its integrity.
- Depending on the criticality of information, data that is required to be checked for integrity shall be selected.
- Periodicity of testing backup is provided in Backup and Restoration procedure.
- To provide assurance that the backup has been completed properly, logging of the backup tasks shall be enabled where possible. Manual backup process shall be logged in a backup register. The backup register shall be reviewed on a monthly basis by the Sr. Manager (IT).

8. OPERATIONAL SECURITY & COMMUNICATION

This section addresses NAVACHETANA need to develop, communicate and implement formal methods and procedures for communication and operation of internal organization and related third party procedures associated with day-to-day administration of information security related areas in Financial Services and management of IT functions.

Documented Operating Procedure

- The operating procedures shall be planned and documented. The jobs in production area shall be planned and scheduled properly.
- The procedures shall contain activities associated with information processing and communication facilities such as access control procedures, back-up procedures, system and network management procedures, asset management and handling procedures etc. All business units in consultation with IT team shall frame the procedures.
- Documented operating procedures such as user manual, technical manual, system architecture and configuration shall be maintained for applications, operating systems, databases and other relevant components as appropriate.

Capacity Management

- New systems shall be tested for capacity, peak loading and stress testing. They shall have a specified and acceptable level of performance, and resilience, which meets or exceeds the hardware baseline as defined. The IT team is responsible for capacity planning.

- System tuning & monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Projections of future capacity requirements shall take into account current & future projected trends.

Malware

- Antivirus application shall be installed on all the systems. IT team shall ensure that any workstation (servers, desktops and laptops) that is connected to the network is installed with the company approved antivirus program. A new system shall be allowed to connect to the network only after it is verified that it has adequate virus protection mechanism.
- Mobile codes such as ActiveX, Java Scripts, Macros etc., shall be controlled within NAVACHETANA and users are encouraged not to use such codes.
- Virus signatures are to be updated on a regular basis. Adequate redundancy mechanism shall be made available to ensure that virus signatures are available if the main sources for providing antivirus updates are not available.
- Any files copied from removable media (CDs / DVDs) shall also be scanned appropriately.
- Any attachment that is received or downloaded shall be appropriately scanned by the antivirus application.

Logging, Monitoring & Clock Synchronization

- NAVACHETANA shall introduce monitoring of systems, servers and other important information processing facilities to detect unauthorized activities from internal and external network and also to ensure information systems problems are identified.
- System monitoring shall also be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.
- Clock synchronization to all the clocks of backend and security systems should be enabled and should be verified periodically.
- Domain server should be designated as the master clock and it should be periodically synchronized with known accurate time source.
- All other system clocks have to be synchronized to the domain server clock.

9. SYSTEM ACQUISITION & MAINTENANCE

Applications provided by partners, vendors and owned by NAVACHETANA are the lifeline of the successful running of processes of NAVACHETANA. Applications include operating systems, infrastructure business applications, off- the-shelf products, services and outsourced applications. It is essential that security is emphasized and insisted from all providers that their products are secure from attacks and failures.

This section describes NAVACHETANA approach to manage application support and maintenance activities that provide adequate controls to ensure confidentiality, integrity and availability of its products. It ensures that a well-defined methodology is adopted for maintenance of applications.

Vendor Provided Applications

- NAVACHETANA as part of the agreement / contract with vendors shall insist or give security requirements and considerations of the products or applications. Essentially, the products should be certified for in-built security considerations. This could include controls against buffer overflow, non-existence of back doors, Trojans, covert channels, etc. The declaration or certification could either be from the customer or vendor or by an accredited third party. Also, in the contracts NAVACHETANA shall insist that only after a formalized testing methodology the product or application will be put to use.
- Any security feature found missing that could affect the business or security of NAVACHETANA should be rectified by the third party. It is also important that provision

of security patches, version change, and product enhancements concerning security shall be provided by the third party as and when required. For products that are already put to use, NAVACHETANA shall insist on a declaration from the third party that all security considerations have been taken into account and the product / application is free from security threats. Wherever applicable, the program or application source code should be requested and stored safely within the premises of NAVACHETANA.

- The service levels and deliverables should be clearly defined, agreed and signed in the agreement. Responsibility matrix for uptime, problem reporting and resolution based on criticality should be defined.

Operational Software

Control shall be provided for the implementation of software on operational systems. To minimize the risk of corruption, the following controls shall be considered by NAVACHETANA:

- Update of operational libraries shall only be performed by the nominated persons
- Executable codes shall not be implemented on operational systems until evidence of successful testing and user acceptance is obtained and the corresponding program source libraries have been updated
- To keep track of users, an audit log shall be maintained
- Previous software versions shall be maintained as a contingency measure
- Decisions to upgrade to new release shall be done after approval from the respective Business unit head. Also, the security level of the patch or new program should be verified for any problems affecting this version and then implemented.

Protection of Test Data

- Access to test data should be provided only after removing the sensitive business and personal information.
- Users should ensure that once the objective of testing the application/data has been met, such data should be deleted from the test application system or move to a secured authorized location.
- Test data should be segregated from operational data. The use and copying of operation data should be logged to provide an audit trail.

Patches, fixes & updates

- A centralized patch management system shall be put in place by IT team to download, analyze, test various patches, fixes and updates released by the vendors and then install them in the applications.
- Any known mal-function operationally and security-wise observed, reported in third party applications has to be reported to the concerned vendors immediately. Any new updates given by vendors have to be version-controlled to prevent attacks.
- In case of proprietary software of vendors, patches and fixes are released by vendor periodically. IT team shall download, test and update the patches as and when deemed necessary.

10.COMPLIANCE & AUDIT

This section lays down the treatment intent towards compliance with contractual, legal and ethical requirements. This policy also ensures compliance of systems and personnel with organizational policies, procedures and standards.

This policy sets out NAVACHETANA's arrangements for avoiding breaches of legal, statutory, regulatory or contractual obligations related to information security and any security requirements and periodical audits towards compliance.

The purpose is to ensure that NAVACHETANA employees, contractors, third party personnel and others who access information or information processing facilities remain compliant with applicable laws, Government directives, contractual obligations, policies, procedures and standards.

Applicable regulations

- Contractual obligations (NAVACHETANA Customers)
- Vendor contracts/agreements
- NAVACHETANA Corporate directives
- Local Laws & Government Directives

Adherence to Policies and procedures

- It is the responsibility of users to adhere to policies and procedures. There shall be regular monitoring of user activities and the violation of policies and procedures shall attract disciplinary action.

- As part of monitoring, management shall carry out periodic audit and inspection to ensure compliance. In this regard, NAVACHETANA may monitor the activities of the end user with the help of logs. To create awareness about policies and procedures NAVACHETANA shall conduct appropriate training sessions for users.
- All emails shall have disclaimers, to protect the organization from any loss that may result from inappropriate usage of the email by the sender or the receiver.

Information systems audit considerations

- Information security stand point of NAVACHETANA shall be audited periodically as per the approved audit calendar by competent personnel who are independent of the activities being audited.
- Reasonable resources for performing audits and reviews (such as access to systems, data, technical staff, procedures, and any special processing or reports) must be identified by the auditors, agreed and made available by management.
- Owners of the audit tools, software and associated data must ensure that they are suitably protected against unauthorized access to prevent any possible misuse or compromise.
- Procedures related to audit is given in - Monitoring and Audit Procedure.

Protection of records

- NAVACHETANA shall ensure that important records including personally identifiable information shall be protected from loss, destruction and modification. The records are to be retained according to the contractual or business requirements.
- The retention period is decided based on the requirements and appropriate care shall be taken to protect the documents from damage and unauthorized access.

Adherence to agreements

- NAVACHETANA shall ensure compliance with any agreement it has signed with other entities. Usage of third-party information shall be strictly in accordance with the agreement and any applicable regulatory and legal requirements.
- Compliance with contractual obligations signed with the suppliers shall be monitored and complied with to prevent any legal proceedings/penalties.

Copyright

Infringement of copyright is a criminal offence. NAVACHETANA employees should be aware of, and should comply with, the contractual provisions in this regard.

Software licensing legislation

Copying and distributing licensed software is illegal, unless the owner of the software expressly grants permission. The following should be considered while implementing the policy:

- Software shall not be copied and distributed across the computer network the violation of which may lead to legal action.
- Use of unlicensed software by contractors and consultants on NAVACHETANA premises should be prohibited, as it could result in legal action against NAVACHETANA.
- Software licenses, paper & electronic copy, shall be kept in safe custody, and if required, shall be produced for inspection.
- Strong internal controls should be implemented to ensure that the maximum number of permitted user licenses is not exceeded.
- Resale of old or redundant computer equipment can result in infringement of the copyright law, as software license agreements may not be transferable; so all the software on the storage media shall be expunged.
- Shareware / freeware software shall not be used.
- Cracking or breaking the licenses of software is prohibited.
- Software license contracts must be renewed on time.

Independent review

Scheduled, periodic review

The control objectives, controls, policies with supporting guidelines, procedures and processes shall be independently reviewed once in a year to ensure their completeness, effectiveness and usability.

Unscheduled review

The CISO will also review control objectives, controls, policies with supporting guidelines, procedures and processes in response to any changes affecting the basis of the original risk assessment such as organizational changes, technological changes, significant security incidents, new vulnerabilities, etc.