LODHA
BUILDING A BETTER LIFE

Information Security Policy

V2.1 Date May 2022

Policy Statement

At Lodha, we create, receive, process, store and share information about ourselves and our clients. Understanding the threats to that information and how we can protect it is vital to the continued success and profitability of our company. This Information Security Policy and its supporting Standards describe the measures we must all take to reduce the risks to that information.

Context

Information Security means making sure that our information can only be accessed by those who have a legitimate business need for it; is protected from unauthorized or unintended changes and is available to those who need it, when they need it. This is known as confidentiality, integrity and availability (CIA).

With heightened government security regulations and the increased threat of cyber breaches, it is more important than ever that our actions do not expose information to unauthorized disclosure, loss or destruction.

Scope

This Policy establishes the minimum requirements and behaviors for Lodha Associates. Stronger controls may be required in some cases (e.g., to meet legal or regulatory requirements), but these are NOT part of the Lodha Information Security Policy.

It applies to all parts of Lodha globally, including subsidiaries, Lodha associates, contractors, temporary staff, contingent workers and anyone else who has access to the Lodha network or systems. It applies to all information processing facilities, premises, systems and networks operated by or on behalf of Lodha. Third party suppliers who process information on our behalf will be expected to have security controls that mitigate information security risks to at least the same level as this Policy.

This Policy shall annually be reviewed, assessed and updated as necessary by the CIO or his or her qualified designee.

Roles and Responsibilities

Everyone at Lodha has an active role to play in ensuring the security of information in accordance with this Policy and any other associated guidance that may be issued from time to time.

Information Security at Lodha is built on the principles of Aware-Protect-Report:

- **Aware** – the information security requirements and behaviors expected of Lodha associates by reading this Information Security Policy and taking the mandatory training, you will be given.
- **Protect** – Lodha information and that of our clients, your associates and yourself by following those requirements and displaying those behaviors.
- **Report** – any information security incidents or suspicious activity by following the Lodha cyber-security incident response process.

Contents

1. Classification and labelling of information

Classification

At Lodha, all information will fall into one of three **Classifications:**

Unrestricted: Information that is publicly available or whose release or publication to any individuals and entities outside of Lodha has been approved For example:

- Published press releases, published market reports, published marketing materials in general circulation and published Lodha financial information.
- Information on the public Lodha websites or Lodha social media accounts.

Confidential: Information that is more sensitive than 'Unrestricted' but does not meet the criteria to be classified as 'Highly Confidential'. If disclosed, 'Confidential' information would only cause minor damage or loss to Lodha or our clients.

This is the default classification for Lodha and client information and covers most information processed by Lodha including:

- General correspondence and business records.
- Internal communications for Lodha staff.
- Policy and Standards documents and operational procedures.

Highly Confidential: Information for which unauthorized disclosure or compromise could cause significant damage or loss to our clients, Lodha or other persons including our associates, and information where disclosure or compromise would be reportable externally to regulators or other bodies.

Examples include:

- Personal Information relating to identifiable individuals, including personal client and colleague information as defined by the Lodha Privacy Policy.
- Unpublished company results.
- Information contained in employment agreements with Lodha associates.
- Information contained in contracts and non-disclosure agreements (NDAs) with clients or other parties.
- Information that is highly restricted by legislation or which, if disclosed, could compromise a client's insurance cover.
- Board-level information and business plans, such as M&A activities, senior hires, etc.
- Information on legal proceedings, regulatory and E&O (errors and omissions) matters.
- Some security configuration and controls documentation.
- Credit card or payment card information.
- Intellectual Property (IP) and Proprietary information.

Note: Where information of different classifications is aggregated then it must be treated as if it is all of the highest classification and handled accordingly.

Labelling of information

To ensure associates are made aware of the sensitivity of the information they are handling, information classified as Highly Confidential and Confidential must be labelled accordingly. There is no requirement to label Unrestricted information.

2. Information security incidents or suspected information security incident reporting

Despite our best endeavors, sometimes information security incidents do happen. When they do, it is critical that they are reported immediately. This allows us to manage the incident and minimize the impact, as well as reduce the likelihood of a recurrence.

Information security and data loss incidents must be reported immediately to:

- ✓ Your local IT Service Desk
  - via their normal contact methods
  - or by email to security.incidents@lodhagroup.com
- ✓ You should also advise your line manager

Reportable incidents include:

- Actual incidents, where a data loss or compromise has occurred, even if the data has subsequently been recovered.
- Near misses, where an incident could have occurred but other internal controls or action by you or others prevented it from happening.
- Any occasion where you are asked to ignore the requirements of this Information Security Policy, even if there is a justification for the request.

You must NOT discuss actual or suspected information security incidents with clients or other third parties unless you have received explicit permission to do so from Information Security.

Please refer the Information Security Incident handling process for more details.

3. Personal awareness and training

Lodha provides a range of resources to help associates understand our expectations for security of information and how to work securely. You are personally responsible for:

- ✓ Reading, understanding and complying with this Policy.
- ✓ Staying up to date with any changes to this Policy, or other security requirements as notified to you from time to time.
- ✓ Completing in a timely manner all mandatory Information Security awareness training activities that are assigned to you.
- ✓ Requesting additional support, guidance or training if you feel you need it.

4. Treating information appropriately

You are responsible for how you process, store and share information throughout its lifecycle from its creation to its secure destruction.

It is Lodha policy that you:

- ✓ Do not share your passwords or Personal Identification Numbers (PINs) with anyone.
- ✓ Only conduct business on properly secured computers and devices as approved by Lodha.
- ✓ Only share information when authorized to do so, and let recipients know if it must not be circulated further.
- ✓ Do not store Lodha information or conduct Lodha business using personal IT equipment or services, other than through methods officially supported or approved by IT

- ✓ Understand the importance of all Lodha information you come into contact with and protect it in accordance with the Lodha Information Classification scheme as described in Section 1 above.
- ✓ Do not attempt to access information if access has not been approved and provided to you, or if you do not need to see it.
- ✓ Destroy information that is no longer required by following Lodha's approved methods such that it cannot be recovered or reconstituted.

5. Access and use of information systems

Lodha provides access to computer equipment, the Lodha networks, and certain external services to support you in your work for Lodha.

You must not:

- ✓ Use Lodha facilities for running or managing any personal businesses, (reasonable personal non-business use is permitted where such use does not interfere with your ability to perform your role).
- ✓ Take any action that could compromise the security of our systems or information.
- ✓ Change the configuration of your computing devices unless approved by IT. This includes attempting to bypass controls, turning off or disabling security features, installing unapproved software or removing mandatory software.

You must:

- ✓ Immediately report any abnormal behavior of your workstation or systems to your IT Service Desk, as this may indicate the presence of malware.
- ✓ Immediately report to your IT Service Desk any information security control that you identify as not working properly or effectively.
- ✓ Immediately notify your line manager or your IT Service Desk if you discover that you have access to resources that you are not authorized to access.
- ✓ Consult your line manager if you are unsure of the levels of authorization you should have on systems or to information.

6. Sending information by email and use of the Internet

Internet and email access are provided for work purposes.

Access to your personal email accounts (eg *me*@hotmail.com) from Lodha provided computers is not permitted.

Some reasonable and appropriate personal use of Lodha provided internet and email services is acceptable. Please remember that this is a privilege that can be withdrawn if abused.

Emails and attachments can be designed to compromise your security or infect your computer, but even normal use of email can create risk for Lodha unless the following requirements are observed:

- ✓ Exercise caution with emails and attachments even if they appear to come from a trusted source, but especially if you are not expecting them or they are from senders you do not know.

Before sending information by email, check:

- ○ You have selected the correct recipient(s).
- ○ All email addresses are correct.
- ○ All recipients are entitled to the information.
- ○ You are only sending information that the recipient needs.
- ○ You have attached the correct documents.
- ○ The correspondence presents both yourself and Lodha in a professional light.
- ○ The information is protected and sent in accordance with the Information Handling Instructions.

- ✓ Exercise caution before clicking on links within emails, even if they appear to come from a trusted source. It is always safer to type the full web address (URL) manually rather than clicking a link, as a link may be sending you to a malicious website without you being aware.
- ✓ If you think you may have received a malicious email follow the incident response procedures in Section 3.
- ✓ You must not send Lodha information to your personal email accounts or unapproved file sharing services (such as Dropbox); do not set your Lodha email to autoforward to your personal external email account, or any other unauthorized external email account. Please use SFTP mechanism to transfer files between customers/Vendors for business purpose.
- ✓ You must not use your personal email accounts to transact business on behalf of Lodha.
- ✓ If you are asked to send business information to a client or other external party, you must only send it to their official address.
- ✓ Information must be sent in accordance with the Information Handling Instructions.
- ✓ If you email an encrypted file, the password must be provided to the intended recipient via a separate media, for example in person or by phone, NOT by email.
- ✓ Do not send, forward or respond to junk mail, 'joke' messages or chain letters.
- ✓ If you are using 'reply to all', or replying to emails where you have been blind copied (bcc), make sure that your responses are suitable for the entire audience.
- ✓ Lodha deploys software that prevents access to most malicious, offensive or illegal websites but no software is 100% effective. Therefore, you must exercise caution when browsing the web, and should you accidentally visit a web site that you feel may be considered inappropriate, leave it immediately.

How to spot a 'Phishing' attempt 'Phishing' is where someone sends you an email and tries to persuade you to click a link or share information when you usually would not.
Phishing emails can be hard to spot. Some signs include:

- Requests you didn't expect
- Links to unexpected web sites
- Unprofessional language, poor spelling or bad grammar
- Emails to multiple recipients
- Software downloads
- Virus warnings
- Emails from an unusual address
- Requests for money or help
- Requests to provide passwords or bank details to a website

Vishing and Smishing
In the same way as phishing, uses email to try and persuade you to share information when you usually would not, vishing and smishing use phone calls and text messages to try and catch you out.
Before responding to unexpected calls or texts verify:

- The identity of the caller/sender
- The authenticity of the request

If you are in any doubt, ask for contact details and only communicate with them once you have confirmed the number is legitimate.

7. Mobile devices

Lodha allows associates to use mobile devices to access emails on their smartphones and tablets

When using mobile devices, you should be aware that:

- ✓ Lodha policies still apply.

8. Portable storage devices (such as USB, SD cards, CDs)

Portable media such as USB, CDs and portable hard drives may not be used to store or share information rated as Confidential or Highly Confidential, unless Information Security has approved the use and other more secure means are not available.

If you do have approval, Confidential or Highly Confidential information must be encrypted using Lodha approved software or tools as provided by your IT department.

You are responsible for the security of the device, and any data on it, until it is returned or until the data is securely deleted. You must ensure that:

- ✓ Use of portable media is restricted to those who require it for business purposes.
- ✓ Devices are not used to transfer files to a personal or home computer.
- ✓ You have permission to copy and share any files before you do so.
- ✓ You securely delete the data on the device once it is no longer needed (your IT team or the Information Security team can advise you how to do this).
- ✓ Passwords are not kept with the device.

9. Sharing information online

Social media has emerged to be a dominant force in our lives. It has transformed the way we interact, consume content and engage with the world at large, both as an individual and as a business. Be cautious about your use of social media - what you say online reflects on you personally and Lodha as a whole.You must act on social media in a manner that does not: put Lodha or our clients at risk; violates legislation or regulations; or impacts the reputation of Lodha or our clients.

Lodha information may not be shared on social media other than as part of authorized activity (such as approved marketing exercises). Information classified as Confidential or Highly Confidential must never be shared on social media without explicit approval from the information owner.

When using your own social media sites or accounts, remember to:

- Be careful with what you share. Anything you put online can be there forever.
- Check the security settings of your social media profiles so you know who you are sharing information with.
- Avoid placing your own sensitive information on social media sites. Information such as locations, birth dates, employment information or friends and family may seem harmless, but can be used maliciously.

Please refer the Social Media Policy for more information about posting contents on Social Media.

10. Securing your computer, user accounts and passwords

Your login accounts are individual to you and you may not share them with anyone else under any circumstances. It is important to keep your password secure as you will be held responsible for any activity performed by your account. You are expressly forbidden from logging into computer systems using another colleague's login account, and from accessing computer systems via a colleague's logged in account.

- ✓ Always lock the screen of your computer before you leave it unattended.

- ✓ Keep your passwords and Personal Identification Numbers (PINs) confidential and do not share them under any circumstances. You will not be asked for your password by Information Security, IT or management.
- ✓ In many cases your password format is controlled by the systems you use, but if not then your passwords must have at least ten characters and include at least three from: numbers, capital and lower case letters and special characters. (See box for advice on choosing a strong password).
- ✓ Consider using longer and more complex passwords depending on the criticality of, and risk to, the information being protected.
- ✓ Network passwords must be changed at least every 60 days, and recently used passwords must not be reused.
- ✓ PINs should always be at least 4 digits.
- ✓ You should try to memorize your passwords and PINs. If you are unable to do so, do not write them down insecurely. Contact IT or Information Security for advice.
- ✓ If you believe your password or PIN has been compromised, change it immediately.
- ✓ You must follow the information security incident response process (refer to Section3 above) if you:
  - ✓ Are asked to share your password or PIN with someone else
  - ✓ Are asked to enter it unexpectedly, for example into an external web site
  - ✓ Believe your password or PIN may have been compromised.

Tips for creating a strong password

- Easily-guessed passwords such as 'Password1' and 'Abcde2022' are not good choices. Other examples that are easy to guess are your office location, the month, celebrity names, dictionary words or the names of family members.
- Use capital letters and numbers in the middle, rather than the beginning and end.
- Don't just add a number at the end of a password and increment it every time you change it.
- One good way to create a password that is both memorable and hard to guess is to use a phrase and take the first letter of each word.
- Another way is to combine two or more words that do not normally go together, and add numbers and punctuation marks.
- Use different passwords for different websites. Do not use your Lodha network password for anything else.
- Never use the same password or PIN you use for personal banking.

Remember your password is only secure if you keep it to yourself.

11. Sending information by fax

Fax is not a secure means of sharing information but is still in use by some clients and suppliers. Generally, use of fax should be avoided because the information is not encrypted, it is easy to enter the wrong number, and there is no guarantee that the intended recipient will collect the document.

If you need to send information by fax, ensure that you:

- ✓ Do not send information classified as Confidential or Highly Confidential unless this is the only method available.
- ✓ Obtain approval from the Client before sending them Highly Confidential information by fax.
- ✓ Collect information that has been faxed to you immediately.

Before sending information by fax, check:

- The person you are sending the information to is available to collect it.
- You have confirmed the number with the recipient.
- You have entered the number correctly.
- You are only sending information that you intended and have not picked up any additional documents.
- There is no other means of sharing the information and you have approval if required.

After sending the fax, check:

- Documents have not been left on the fax machine.
- Confirmation notices have been collected.
- The intended person has received it.

12. Access to premises

Lodha operates physical security controls in all our buildings, with which you must comply. In particular:

- ✓ You are responsible for the actions of visitors you invite onto Lodha premises.
- ✓ Do not leave visitors unattended.
- ✓ If you see someone you do not recognize, offer to help them. If they are a visitor, escort them to their host or reception. If they claim to be a colleague, you are entitled to confirm this.
- ✓ Do not attempt to follow someone else through a security gate without presenting a valid pass ('tailgating').
- ✓ Be aware of unauthorized persons attempting to follow you.
- ✓ Follow agreed procedures when working in areas designated as 'secure' or 'confidential'.
- ✓ Report any unusual behavior to your building security team or line manager.
- ✓ If you lose an identification badge you have been given, you must immediately inform your Facilities Manager or local reception desk.
- ✓ Additional controls must be in place to secure critical or sensitive information. Access to secure areas must be strictly restricted e.g. Access to server rooms must be controlled and restricted to an authorized personnel (like Engineers, Server/Database/Network administrators) who need to perform their duties.
- ✓ Signs indicating "Authorized Personnel Only" or a similar message should be prominently posted at all entrances of secure areas.
- ✓ Knowledge or access of the "secure areas" (example: server room, UPS room, etc) should be given to associates or third party on a "need-to-know" basis.
- ✓ Server rooms must not be visible or identifiable from the outside i.e. there should not be any window or directional signs providing access to such rooms.
- ✓ Appropriate access controls and segregation of duties shall be enforced to ensure confidentiality and integrity of the data residing in each of the setup.

13. Working out of the office (including while working at home)

You should be cautious and vigilant when working out of the office. Screens and documents can be easily viewed, and discussions or phone calls can be overheard.

Secure mobile working facilities are provided for your use, including email and remote access to the Lodha network.

- ✓ Only use Lodha approved remote access solutions to access our information.
- ✓ Never leave computer equipment unattended when working away from Lodha premises.
- ✓ Always use the screen-lock when away from your computer.
- ✓ Never leave documents unattended when working away from Lodha premises and always put them out of sight when no longer in use while working at home.
- ✓ If travelling by air or public transport, equipment and documentation must stay with you as hand luggage at all times. They must not be placed in the hold of an aircraft.
- ✓ If travelling by car, do not leave equipment or documents on display, and where possible lock them securely in the trunk or boot of the car before travelling. Do not leave them in the vehicle overnight.
- ✓ Printed documents must be securely disposed of by cross-cut shredding, or returned to a Lodha office for secure disposal.
- ✓ Exercise caution when using public WiFi hotspots or other untrusted networks. These networks may be accessible to malicious users. Use a mobile data connection such as 3G, 4G or 5G wherever possible.
- ✓ When using a wireless connection at a hotel or public place, confirm the name of the wireless network that should be used to avoid rogue wireless connections.
- ✓ Where there is reasonable risk from your laptop being overlooked, use a privacy screen to protect it.

14. Security of printed documentation

Lodha operates a 'clear desk' policy which means that Confidential and Highly Confidential information must not be left in unlocked meeting rooms and open areas at any time.

When you are away from your work area during office hours, Confidential and Highly Confidential information must be out-of-sight. At the end of the working day, Confidential information must be put away (preferably locked away) and Highly Confidential information must be locked away in desk drawers, filing cabinets or filing rooms.

Remember:

- ✓ Avoid printing Highly Confidential information unless absolutely necessary.
- ✓ When you print, if the printer does not support "authentication prior to printing", collect your document immediately. Do not leave documents on shared printers.
- ✓ Avoid taking documentation classified as Confidential or Highly Confidential out of the office unnecessarily.
- ✓ Only retain printed documentation for as long as it is needed and then securely destroy it.
- ✓ Where possible avoid sending information classified as Confidential or Highly Confidential in the mail.
- ✓ When hardcopies of Highly Confidential information must be sent by mail in bulk (e.g. transferring paper files) permission must be obtained from the client (or information owner if it is Lodha data) and they must be sent by an approved courier with receipt confirmed.
- ✓ Dispose of information classified as Confidential or Highly Confidential in the secure disposal facilities or shredding bins provided in your offices.

15. Document retention

It is important that Lodha has access to information you use or create for only as long as we need it. You must:

- ✓ Store electronic information only in approved document and record management systems (such as the Team Collaboration Tool) or appropriately secured applications or file shares. If you temporarily have to store information locally (such as on your Lodha laptop if working remotely), transfer it to the appropriate network location as soon as possible.
- ✓ Ensure your associates know where to find information they may need, e.g., by following the Records Management Standards, Guidelines and recommendations on filing.
- ✓ Be careful not to delete information that may still be required.
- ✓ Securely archive data that must be retained but is not required for immediate use and follow the Records Management Guidelines for archiving paper files wherever possible.
- ✓ Securely dispose of data when it is no longer required. Follow the Records Management Standard on shredding wherever possible.
- ✓ Retain information that is subject to a legal destruction hold order.

16. Network Security

As mentioned in Section 10, Network authentication is provided by Username and password for individual users and firewall enforces access policies such as what services are allowed to be access to each network users. The following security measures are implemented to make sure our network is secure

- ✓ Remote access is provided only to the specific systems/host for a specific period.
- ✓ Networks are segregated and L3 Switches/Routers are used to control access to secured systems
- ✓ Application Access Control
- ✓ Access Control on Files and Folders
- ✓ Minimize Single Point of failures and number of entry points to the network
- ✓ Enterprise Authentication mechanism for Wireless networks
- ✓ Device security is maintained by security updates and patches
- ✓ Access to internet based on the work nature of the employee.

17. Expectations of managers

As a manager, you are responsible for supporting your team in adhering to this Policy and any information security requirements notified to you by Information Security. This includes any contractors and third parties you may use who have access to Lodha systems and data. In particular:

- ✓ You must ensure the information security incident reporting procedure (see Section 3) has been followed if a member of your team advises you of an information security incident. If a member of your team advises you that they have accidentally accessed an inappropriate web site as covered by Section 7 you must ensure IT Servicedesk is advised.
- ✓ You must ensure that your team understands Lodha's information security requirements and have completed any training allocated to them.
- ✓ You are responsible for ensuring that staffing changes such as new joiners, internal transfers, changes in role, extended absences and staff leavers (including for contract and temporary staff), are notified in a timely manner so that access can be amended or removed.
- ✓ You must ensure that your team members have the access they need to do their job, and are removed from access they should not have.
- ✓ You must respond to and undertake access reviews for your team in a timely manner, as required by local management or Information Security.
- ✓ If you are a designated information owner, undertake periodic reviews to confirm who has access to your information.
- ✓ If you are a designated information owner, then you must follow the requirements in the Information Handling Instructions.

You must notify Information Security:

- ✓ Of any role conflicts that create information security risks (for example where a transaction could be processed and authorized by the same person).
- ✓ When your team plans to work with a new external supplier (a 'third-party processor') who will process or store information for Lodha or our clients.

18. Secure systems

If you are responsible for the commissioning, purchase or design of information systems and applications, security and data privacy must be considered an integral part from their acquisition and/or development and throughout their lifecycle.

- ✓ Required levels of confidentiality, integrity and availability of information must be considered when specifying requirements for new systems and applications, and whenever significant changes are implemented.
- ✓ Security requirements must be included throughout the lifecycle of all system/software development procedures used by Lodha, whether the development is performed 'in house' or outsourced to a third party.
- ✓ All versions of systems, applications and environments (not just 'production' versions) including testing procedures and the security of test information must have security controls commensurate with the risk.

19. Information security and compliance monitoring

To the extent permitted by local legislation, works agreements and regulation, Lodha will monitor your access to and use of our systems, networks and information, for security, compliance, operational and training reasons. Monitoring may include:

- ✓ Monitoring and reviewing internet use.
- ✓ Monitoring and reviewing your use of email and instant messaging.
- ✓ Tracking access, sharing and modification of files and information.
- ✓ Monitoring your use of computer equipment and services provided by Lodha.
- ✓ Tracking use of resources, such as printing.
- ✓ Monitoring your access to Lodha networks, buildings and facilities.
- ✓ Monitoring use of mobile devices and remote access to Lodha resources.

Subject to the requirements of local legislation, works agreements and regulation, there should be no expectation of privacy on work or personal matters when using Lodha's systems and resources.