GANESH HOUSING CORPORATION LIMITED

POLICY ON CYBER SECURITY

(W.E.F 01/04/2022)

Corporate Identification Number [CIN]: L45200GJ1991PLC015817
Registered Office: Ganesh Corporate House, 100 Feet Hebatpur Thaltej Road,
Near Sola Bridge, Off S. G. Highway, Ahmedabad 380 054

GANESH HOUSING CORPORATION LTD.

Dalal

CHAIRMAN

POLICY STATEMENT

At Ganesh Housing Corporation Ltd. [GHCL], 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 successand profitability of our company. This Cyber 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, lossor destruction

ROLES AND RESPONSIBILITIES

Everyone at GHCL 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 GHCL is built on the principles of Aware-Protect-Report:

- **Aware** – the information security requirements and behaviors expected of GHCL associates byreading this Information Security Policy and undergo training, if required.
- **Protect** – GHCL information and that of clients, associates and by following those requirements and displaying those behaviors.
- **Report** – any information security incidents or suspicious activity by following the GHCL cyber- security incident response process

GANESH HOUSING CORPORATION LTD.

CHAIRMAN

CONTENTS

GANESH HOUSING CORPORATION LTD.
Dalali
CHAIRMAN

1. Classification of information

Classification

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

1] Unrestricted: Information that is publicly available or whose release or publication to any individuals and entities outside of GHCL has been approved.

For example:

Published press releases, published market reports, published marketing materials in general circulation and published GHCL financial information.

Information on GHCL websites or GHCL social media accounts.

2] 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 GHCL or our clients.

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

General correspondence and business records.

Internal communications for GHCL staff.

Policy and Standards documents and operational procedures.

3] Highly Confidential: Information for which unauthorized disclosure or compromise could cause significant damage or loss to our clients, GHCL 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.
- Unpublished company results.
- Information contained in employment agreements with GHCL associates.
- Information contained in contracts and non-disclosure agreements (NDAs) with clients or other parties.
- 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.

GANESH HOUSING CORPORATION LTD.

CHAIRMAN

- 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.

2. Personal Awareness and Training

GHCL 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.

3. 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 GHCL 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 GHCL.
- ✓ Do not store GHCL information or conduct GHCL business using personal IT equipment or services.
- ✓ Understand the importance of all GHCL information you come into contact with and protect it in accordance with the GHCL Information Classification.
- ✓ 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.

4. Access and use of information system

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

GANESH HOUSING CORPORATION LTD.
Dalal
CHAIRMAN

You must not:

- ✓ Use GHCL 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 personal, 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 IT Service Desk if you discover that you have access to resources that you are not authorized to access.

5. Sending information by email and use of internet

- ✓ Internet and email access are provided for work purposes.
- ✓ 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.
- ✓ 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 immediately inform IT team.
- ✓ You must not send GHCL information to your personal email accounts or unapproved file sharing services (such as Dropbox); do not set your GHCL email to auto forward to your personal external email account, or any other unauthorized external email account..
- ✓ You must not use your personal email accounts to transact business on behalf of GHCL.
- ✓ If you are asked to send business information to a client or other external party, you must only send it to their official address.
- ✓ 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.

GANESH HOUSING CORPORATION LTD.
Dalal
CHAIRMAN

- ✓ 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.
- ✓ GHCL 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.

6. Mobile devices

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

When using mobile devices, you should be aware that:

- ✓ GHCL policy still applies.

7. Portable storage devices (such as USB devices, etc)

Portable media such as USB 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.

8. 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 GHCL as a whole. You must act on social media in a manner that does not: put GHCL or our clients at risk; violates legislation or regulations; or impacts the reputation of GHCL or our clients.

GHCL 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.

GANESH HOUSING CORPORATION LTD.

CHAIRMAN

- ✓ 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.

9. Securing your computer system, user account and password

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.
- ✓ 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.
- ✓ 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.

10. Access to premises

GHCL 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 GHCL 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.
- ✓ Be aware of unauthorized persons attempting to follow you.
- ✓ Report any unusual behavior to your building security team Departmental Head.
- ✓ If you lose an identification badge you have been given, you must immediately inform your Facilities HR (Manager).

GANESH HOUSING CORPORATION LTD.
Dalal
CHAIRMAN

- ✓ 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.
- ✓ 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

11. Working out of office [including work from 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 GHCL network.

- ✓ Never leave computer equipment unattended when working away from GHCL premises.
- ✓ Always use the screen-lock when away from your computer.
- ✓ Never leave documents unattended when working away from GHCL premises and always put them out of sight when no longer in use while working at home.
- ✓ Printed documents must be securely disposed of by cross-cut shredding, or returned to a GHCL office for secure disposal.

12. Network security

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.

GANESH HOUSING CORPORATION LTD.

Dalal

CHAIRMAN

13. Expectation of Presidents

As a president, you are responsible for supporting your team in adhering to this Policy and any information security requirements notified to you. In particular:

- ✓ You must ensure the information security incident reporting procedure 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 you must ensure IT Departmental Head is advised.
- ✓ You must ensure that your team understands GHCL'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 created, 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.

14. 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 GHCL, whether the development is performed 'in house' or outsourced to a third party.

15. Information systems and compliance monitoring

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

GANESH HOUSING CORPORATION LTD.
Dalal
CHAIRMAN

- ✓ 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 GHCL.
- ✓ Tracking use of resources, such as printing.
- ✓ Monitoring your access to GHCL networks, buildings and facilities.
- ✓ Monitoring use of mobile devices and remote access to GHCL resources.

GANESH HOUSING CORPORATION LTD.
Dalal
CHAIRMAN