InfoSec Team – Global Information Security Policy

GLOBAL INFORMATION SECURITY POLICY

Global Information Security Policy

01-Apr-20 Version 2.0

FutureBridge

Contents

1. PURPOSE

Information is one of our most valuable assets, and hence we have designed and implemented policies and programs to protect it as per best global practices and standards. Information has many forms including but not limited to physical, document-based, electronic, digital and verbal, and many formats including but not limited to content, data, documents, records, email, user credentials, usernames, user passwords, databases, voicemail, websites, paper-based communication, print-outs, photos, videos, software, software codes, and any other electronic formats. Whatever its format, our information must always be appropriately handled and / or protected.

We need to ensure that all information is sanitized and disseminated on a strict need-to-know basis, and only with prior approvals from its authorized owners and / or authorised users. In particular, we safeguard all information belonging to the Company and all its stakeholders, including but not limited to clients, suppliers, subcontractors and other third parties within a secure environment.

2. DEFINITIONS

For the purpose of this InfoSec Policy:

- '**Company**' shall mean Cheers Interactive (India) Private Limited, its subsidiaries, affiliates and any / all brand names it trades/ shall trade under.
- '**Information**' shall mean all information, whether physical, document-based, electronic, digital or verbal, including but not limited to documents, records, databases, content, data, email, user credentials, usernames, user passwords, voicemail, websites, paper-based communication, print-outs, photos, videos, software, software codes, any other electronic format/s owned by and / or handled by and / or known to the Company, whether or not confidential information and / or personal information.
- '**Confidential Information**' shall have the same meaning as the respective Non-Disclosure Agreement signed by the Personnel.
- '**Computer System**' shall mean any information processing or computing device belonging to the Company including but not limited to desktop computer and / or laptop and / or servers and / or tablet and / or mobile phone.
- '**Electronic Device**' shall mean any device used for the purpose of electronic and / or digital computing, processing, printing, scanning, storage, distributing, disseminating, audio and / or visual photography / recording, audio and / or visual playback. This includes but is not limited to computers, laptops, storage devices, pen drives, external hard disks, memory cards, servers, network equipment, satellite communication devices, telephones, mobile phones, tablets and cameras.
- '**Information Systems**' shall mean the Company's Computer System/s, Electronic Devices, computing systems, information processing systems, electronic information systems (software, computers and peripherals), whether deployed / accessed on or off the Company Premises; information storage systems including but not limited to The Cloud and other storage owned and / or availed by the Company; Company's computer network, whether used directly or indirectly; hardware, software and data owned by the Company; paper-based materials; electronic recording devices (video, audio, CCTV systems, biometrics).

- ‘**The Cloud**’ shall mean a data storage center and / or storage server, whether or not owned by the Company, which is used by the Company to store, maintain and manage data, to back up data remotely, and to access and / or make such data available to users over the internet or an intranet.
- ‘**Commercial Business Premises**’ shall mean any / all the commercial business premises, of the Company, irrespective of its geographical location.
- ‘**Premises**’ shall mean any and / or all premises from where the Company and / or its authorized representatives access the Information to carry out Services for and / or on behalf of the Company. Premises may or may not be owned by the Company (whether partly or in full) and shall include, but not be limited to, the Commercial Business Premises mentioned above, any other business premises, rented premises, retail premises, temporary premises, warehouses, manufacturing units, storage facilities, shared commercial premises, shared office premises and / or hubs, home-based premises, premises from where an authorized representative accesses the Company’s data remotely, onsite and / or offsite physical storage premises and / or The Cloud.
- ‘**InfoSec Policy**’ shall mean this Information Security Policy.
- ‘**Laws**’ shall mean all applicable local, state and international laws, including laws of all the countries where the Company operates.
- ‘**Personnel**’ shall mean the directors, officers, employees, consultants, subcontractors, contractors, vendors, suppliers and agents of the Company, and / or any other third parties who engage with the Company and / or have access to the Information and / or Information Systems of the Company, whether or not from the Premises .
- ‘**Critical Network Equipment**’ shall mean those equipment that ensure that all Company’s relevant Information Systems, devices and assets are connected to the Company’s network and / or server at all times, and that Information transfer / transmission between the said relevant Information Systems, devices and assets is continuous and without hindrance. Critical Network Equipment shall include but not be limited to firewalls, core switches and routers.
- ‘**Data Centre**’ shall mean a large group of networked computer servers used by the Company for storage, processing and / or distribution of large amounts of data, whether or not remotely.
- ‘**Whitelisted Email**’ shall mean those email ids which have been expressly authorized by the Company for the permitted purpose of official electronic communication.
- ‘**Blacklisted Email**’ shall mean those email ids which have been blocked by the Company, and sending emails to whom is expressly prohibited.
- ‘**Internal Application / Software**’ shall mean all the applications and software developed by the Company, whether partly or in full, for its internal usage (including but not limited to operational usage), and shall include but not be limited to BD software, BD collaterals, OPS software, client portals, client communication systems, human resource management systems, program management systems, workflow management systems and knowledge banks.
- ‘**Remote Access**’ shall mean an authorized external connection by an electronic device / host to Company’s authorized data network to access Information Systems owned, managed and / or maintained by the Company.
- ‘**We / Us / Our**’ shall mean the Company and / or the Personnel of the Company, and / or any other third parties who engage with the Company and / or have access to the

Information or Information Systems of the Company, whether or not from the Premises; both jointly as well as severally.

3. APPLICABILITY

This Policy applies to the Company and all its Personnel and all other third parties who engage with the Company and / or access the Information or Information Systems of the Company, whether or not from the Premises.

4. INFORMATION SECURITY PRINCIPLES

To prevent threats or recover an ecosystem after an incident, Our InfoSec Policy is based on techniques and technologies that aim at the following principles:

- **Confidentiality**: We ensure that Information is only accessed by authorized users having necessary rights on a strict need-to-know basis. We strive to protect all Information from unauthorized disclosures, from loss of or unauthorized viewing, and from data breach;
- **Integrity**: We ensure the correctness of the Information, and take necessary precautions to prevent modification, corruption, damage or destruction of Information and Information Systems;
- **Availability**: We maintain the availability of the Information by protecting it from disruption, and by keeping regular back-ups of all Information.

5. GENERAL OBLIGATIONS OF INFORMATION SECURITY

We shall exercise a duty of care in relation to the operation and use of the Company's Information Systems. Usage by authorized users shall be lawful, honest and decent. We shall ensure that:

- Information is protected against unauthorized access or misuse;
- Confidentiality of Information is secured;
- Integrity of Information is maintained;
- For a reasonable period of time, availability of Information / Information Systems is maintained to the extent required for service delivery;
- Business continuity planning processes are maintained;
- Regulatory, contractual and legal requirements are complied with;
- Physical, logical, environmental and communications security is maintained;
- When Information is no longer of use, it is disposed of in a suitable manner;
- All Information security incidents are duly reported and thoroughly investigated through appropriate channels;
- Information Systems are adequately protected from unauthorized access;
- Information Systems are reasonably secured against theft and damage;
- Adequate steps are taken to ensure the availability of the Information Systems in accordance with its importance, and the business continuity processes of the Company;
- Electronic Information can be recovered to a reasonable extent, in the event of loss of the primary source;

- All relevant Information Systems have provisions for Backup Data, so as to enable the Company to restore Information to a level commensurate with its importance, and its disaster recovery policies;
- Information Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse;
- Any electronic access logs are retained for a justifiable period to ensure compliance with applicable data protection laws;
- Any third parties entrusted by the Company with Information or Information Systems understand their responsibilities with respect to maintaining its security, and have adequate information security measures in place;
- Personnel are prohibited from referencing the subject or content of sensitive Information or Confidential Information publicly, or via systems or communication channels not controlled by Company;
- Personnel are prohibited from storing Information anywhere except on the Information Systems;
- Personnel are prohibited from using any cameras, audio and / or visual recording devices, directly or indirectly, in any way whatsoever, on the Premises and / or during Remote Access, whether or not during the working hours. Such usage shall be considered as an unauthorized usage of Electronic Devices as mentioned in Section 6 hereunder;
- Personnel are prohibited from discussing / exchanging Confidential Information, either publicly or privately, whether or not on the Premises, unless expressly authorized by the Company to do so.

6. SECURITY OF INFORMATION

We shall ensure the security and safety of all Information by adhering to the following:

PERSONNEL ON-BOARDING / ENGAGEMENT

- All Personnel engaged with the Company shall read the InfoSec Policy, and shall make themselves aware of their information security obligations therein.
- All Personnel shall, at all times, be obligated to report security incidents to their department heads and / or to the InfoSec Team at teaminfosec@cheersin.com.
- Each Personnel shall sign a corresponding Non-Disclosure Agreement with the Company.

PHYSICAL SECURITY

Physical security of Information and Information Systems is an important aspect of our Information Security Policy. We shall ensure that:

- Access to Data Centre is restricted to only those Personnel whose job responsibilities require such access;
- Signs are placed at appropriate places, warning that such access is restricted to authorized Personnel;
- Doors to Data Centers are secure, both physically (through various measures including but not limited to installation of surveillance cameras) and digitally (by regulating the entries to / exits from the Data Centre using proximity card readers, and / or through biometric authentication);

- Data Centre have redundant power sources, such as a generator, to power electronic locks and authentication systems in case of a power failure or outage;
- Physical access to the IT Systems is controlled, strictly on a need-to-know basis;
- A system for secure disposal of unwanted discs, tapes, cards, hard drives, printed paper, and anything else that could contain Confidential Information is implemented;
- Fire safety systems are installed at appropriate places;
- Access to work areas is strictly monitored through proximity card readers, and / or through biometric authentications, as appropriate;
- Visitors to Premises shall be escorted by an authorized representative of the Company at all times, and their entry shall be restricted to appropriate areas;
- On his / her last working day and / or on the last day of the engagement, each Personnel shall return all Company property in his / her possession including but not limited to Electronic Devices, print-outs, storage devices, storage media, diaries, books, notepads, documents, data, records, identification / proximity cards in any format, whether or not containing Information.

<u>LOGICAL SECURITY</u>

- <u>Security of Computer Systems</u>

  We aim to keep all our Computer Systems secure according to the best industry standards and practices. We shall ensure that:

  - All Computer Systems have authorized and properly configured operating systems, anti-virus software, security patches, information rights management systems, data loss prevention systems, unified threat management systems, anti-spyware programs and firewalls installed, configured and updated with latest signatures;
  - There are regular checks for (and subsequent application of) vendor security updates for the Operating Systems of each Computer System;
  - Each Personnel should have access to a Computer System with a Windows authentication and a strong password;
  - A Personnel cannot install or download software applications and/or executable files on the Computer Systems without prior written authorization from the Information Security Department;
  - Storage devices including but not limited to Floppy drives, CD ROMS and USB ports are disabled for all Computer Systems;

- <u>Password Management</u>

  In order to provide consistent and secure management of passwords for Personnel and Information Systems, We shall ensure that:

  - All Our Information Systems have secure and unique password credentials;
  - Passwords are complex, and a combination of lowercase letters, uppercase letters, numerals and special characters;
  - Personnel are discouraged from setting passwords containing security-sensitive information / personal information;

- Personnel are discouraged from using the same password for different systems and logins;
- Personnel are prohibited from writing down passwords, or sharing the passwords with any third party, whether or not in writing;
- The Company's IT Team never asks for the passwords of the Personnel, and instead, sets temporary passwords for Personnel who cannot log into the Information Systems due to expired passwords / locked accounts;
- The Computer Systems passwords are periodically changed to protect against unauthorised usage.

- Security of Information Systems

  We keep all Information secure according to the best industry standards and practices. We shall ensure that:

  - Information, is accessed by Personnel only on a strict need-to-know basis for authorised business purposes only;
  - Access to Information on network storage devices is governed by strict access control and audit process;
  - All Personnel having access to Information shall sign strict non-disclosure agreements with the Company;
  - Adequate measures are in place to govern the usage and accessibility of all Information by the personnel;
  - Download of .EXE files of any kind whatsoever is strictly prohibited;
  - Information shall not be stored on local drives of Computer Systems, but on secured and protected network drives;
  - All documents stored in all of the Internal Applications / Software of the Company are secured and protected as per the Company standards;
  - Critical Network Equipment are always placed in the Data Centre;
  - Internal networks are protected by firewalls configured in High Availability Mode and Unified Threat Management Systems.
  - A 'Zero File Upload Policy' is implemented, except to Company's webmail sites and / or to any Whitelisted Emails / domains;
  - All Information stored on The Cloud is adequately protected;
  - Personnel shall have Remote Access only with express written authorization of the Company;
  - Remote Accesses shall be strictly for authorised business purposes only. This InfoSec Policy shall apply to all Remote Accesses locally and globally;
  - Personnel having Remote Access shall prevent access to the Information by third parties of any kind whatsoever;

- <u>Information Rights Management System</u>

  We have an accredited Information rights management system (hereinafter “Information Rights Management System”) in place to protect all our documents stored on our Information Systems. In furtherance of the same, We shall ensure that:

  - All documents stored on the Information Systems that contain Confidential Information are safeguarded, and their access strictly monitored and controlled, by the Company using an Information Rights Management System. Some documents may be additionally protected by a document protection system. Each such document shall be referred to as ‘Protected Document’.
  - Electronic folders stored on the Information Systems that contain Confidential Information are safeguarded, and their access strictly monitored and controlled, by the Company. using an Information Rights Management System. Some folders may be additionally protected by a document protection system. Each such electronic folder shall be referred to as ‘Protected Folder’.
  - Each Personnel may be granted one / all of the following rights to a Protected Document, based on a strict need-to-know and need-for-business basis:
    - View Rights: Rights to only view the Protected Document;
    - View Edit Rights: Rights to view and edit the Protected Document;
    - View Edit Copy Rights: Rights to view, edit and copy paste from a Protected Document to another Protected Document;
    - View Edit Print Rights: Rights to view, edit and print the Protected Document;
    - View Edit Copy Print Rights: Rights to view, edit and copy paste from a Protected Document to another Protected Document, and additional print rights;
    - Print Rights: Rights to view and print the Protected Document;
    - Full Rights: Rights to view, edit and print the Protected Document, and rights to copy paste from the Protected Document to an unprotected document and vice versa.
  - Any Personnel who do not have the necessary rights / who have partial rights to / in a Protected Document as per the Information Rights Management System, shall not be able to access the Protected Document / shall have partial access to the Protected Document, in accordance with the rights he / she / it possesses on the Protected Document;
  - Any third party other than an authorised Personnel shall not be able to access the Protected Document at all;
  - All Functions across the Company shall have designated and separate working folders on the servers (‘**Working Folder**’);
  - A Working Folder can be accessed only by the Personnel on a strict need-to-know and need-for-business basis;
  - Any Protected Document stored in the Working Folder is safeguarded by the Information Rights Management System at all times;

- Any document stored in a Protected Folder is safeguarded by the Information Rights Management System at all times;
- Personnel may have limited rights to the documents, including but not limited to Protected Documents, stored in their respective Working Folder and Protected Folders;
- The rights are determined by the Company in accordance with each Personnel's job specification;
- On a need-to-know and need-for-business purpose basis, Personnel may request the InfoSec Team in writing to provide additional rights to any document / Protected Document;
- All such requests shall be adequately supported by the purpose, the additional rights needed, and the necessary authorization / approvals required;
- Only if the required authorization / approvals are in place, the InfoSec Team shall provide additional rights to the document / Protected Document;
- A document may be shared via email only if the respective Email Id is Whitelisted.
- Blacklisted Email Ids shall be blocked and no Personnel shall be allowed to send any emails to the said Email Ids.

▪ Internet Usage

In order to adhere to appropriate and acceptable internet usage, we ensure that:

- Any uploads on the internet, of any kind whatsoever, for any reason whatsoever, is strictly prohibited;
- All web-based email sites and web-based proxy sites are blocked for everyone in the Company;
- Personnel may be provided professional access to various social networking websites and audio-video websites strictly for business purposes on a need-to-have basis;
- Access of social networking websites, whether permitted or otherwise, shall not conflict with the other obligations of the Personnel, including but not limited to the performance obligations.
- Websites with harmful and / or inappropriate content, including but not limited to network storage websites, pornographic websites, and websites categorized as gambling shall be blocked.

▪ Email Policy

In order to prevent any misuse of electronic mail ('Email'), and the subsequent legal, privacy and security risks, We ensure:

- Email Ids are allotted to Personnel strictly on a "need to use" basis for business purposes;
- Email is configured to send mails internally to all Personnel, and externally to clients, prospective clients and Whitelisted Email Ids only;

- Sending Emails to other Email ids of any kind whatsoever, including but not limited to a Personnel's personal Email id, is disabled;
- Exceptions are allowed on a case-to-case basis, only for business purposes and for a specifically defined time period. In such instances, the Personnel writes an email to teaminfosec@cheersin.com for Whitelisting the required Email Ids. Information security team will whitelist such Email id/s after due investigation and after explicit approval from authorised heads of business / functions;
- The InfoSec Team keeps a record of all such Whitelisted Email Ids, and revokes the exceptions as soon as the required business purpose is over;
- All use of Email must be consistent with Company's Global Code of Conduct applicable to the Personnel, Company's policies, applicable laws and proper business practices;
- The Company email shall not be used for the creation or distribution of any disruptive or offensive messages;

Company may, but is not obliged to, monitor messages exchanged on Company's email without prior notice. Personnel shall have no expectation of privacy in anything they store, send or receive on the Company's email;

- Electronic Device Usage Policy
  - All Electronic Devices, including but not limited to telephones, mobile phones, tablets, laptops and personal computers, shall be used as a communication and / or computing device on the Company's Premises and / or in the proximity of the Company's Information Systems only for purposes permitted by the Company at its sole discretion.
  - Personnel may carry Electronic Devices on the Premises only with the prior express authorisation.
  - All Electronic Devices shall be used only for authorised and / or permitted purposes.
  - Using an Electronic Device's camera or microphone for unauthorised purposes (including but not limited to clicking pictures of and / or recording Information, and screen capture of the Information on the Computer Systems) is strictly prohibited.
  - Personnel shall not use an Electronic Device in areas where its usage is explicitly prohibited.

7. CLEAN DESK POLICY

To improve the security and confidentiality of Information, We have adopted a Clean Desk Policy for work stations. We shall ensure that all Information (whether or not sensitive and / or confidential) on any media, including but not limited to paper, storage media, electronic media or hardware, is properly secured and protected from unauthorized view or access, during as well as beyond a Personnel's working hours, and during periods when workstations / Information Systems are left unattended. Each Personnel shall ensure that:

- All Information in hardcopy or electronic form is removed from the respective workspace and secured in a drawer when the desk is unoccupied and left unattended;
- Computer Systems are locked when the workspace is unoccupied;
- Computer Systems are shut down at the end of the work day;
- File cabinets containing Information are kept locked when not in use or when left unattended;
- Portable computing device are locked in a drawer or secured room;
- Passwords are not written down in an accessible location;
- Printouts containing Information are removed from the printer without undue delay.

8. BACK-UP RETENTION

As a part of Our Back-Up Retention Policy, all information shall be copied onto physical and / or electronic and / or digital back-up media (including but not limited to magnetic tapes and disk-to-disk storage), on Our computer systems (whether or not on the disk) and / or on The Cloud.

We shall ensure that:

- Information stored on local drives is transferred to the protected servers at regular intervals (“**Transferred Data**”).
- All Information on Information Systems which is not required by Personnel, are removed from the regular Information Systems and archived at regular intervals (“**Archived Data**”).
- All essential Information, including Transferred Data and Archived Data, is backed up at regular intervals (‘**Back-Up Data**’);
- Back-Up Data is stored on-site as well as on an off-site location and / or on The Cloud;
- All Back-Up Data is secured and protected by adequate means.
- Access to such Back-Up Data is restricted on a strict need-to-know basis for authorized business purposes only.
- Any retrieval of Back-Up Data shall be expressly authorized by the respective authorized Personnel only.
- Back-Up Data, if retrieved, shall be secured and protected by adequate means, and restricted access shall be granted for limited, specific and authorized usage only.

9. COMPLIANCE WITH APPLICABLE LAWS

We comply, and shall continue to comply with all applicable data protection, data privacy and data security legislations of all countries where We operate, including but not limited to the European Union General Data Protection Regulations 2016/679.

10. AUDITS

We have an audit mechanism in place to periodically check whether all the guidelines mentioned in the InfoSec Policy are complied with by all Personnel.

All Information Systems are audited at least quarterly, in accordance with the Internal Audit Policy of the Company. The records / findings of the audits are maintained and controlled by the Quality System Team. The findings (Internal Audit Reports) are shared with the Management Team as part of the Monitoring and Improvement meetings and appropriate action is taken.

11. NON-COMPLIANCE

We take violations of the InfoSec Policies seriously. Disciplinary actions shall be initiated against any Personnel who violates the InfoSec Policy, including but not limited to a verbal warning, written warning, suspension of services (with or without pay), or termination of employment. In addition, Personnel who violate the Laws mentioned in the InfoSec Policy may also be exposed to substantial civil damages and criminal prosecution.

12. MISCELLANEOUS

The InfoSec Policy is considered an integral part of, and shall be read in conjunction with the other Global Policies of the Company, including but not limited to Company's Global Code of Conduct, as applicable.

[redacted]

[redacted]

[redacted]

North America
55 Madison Ave, Suite 400
Morristown, NJ 07960
USA
T: +1 212 835 1590

Europe
328-334 Graadt van Roggenweg
4th Floor, Utrecht, 3531 AH
Netherlands
T: +31 30 298 2108

United Kingdom
5 Chancery Lane
London EC4A 1BL
United Kingdom
T: +44 207 406 7548

Asia Pacific
Millennium Business Park
Sector 3, Building # 4, Mahape
Navi Mumbai, India 400 710
India
T: +91 22 6772 5700

futurebridge.com

FutureBridge