



Habib Insurance

Information Technology –Acceptable Use Agreement

As a user in Habib Insurance Company Ltd. (HICL) of their local and shared computer systems, you hereby state to understand and agree to abide by the terms of this Acceptable Use Agreement. These terms govern your access to and use of the information technology applications, services, and resources of HICL, and the information they generate and maintain.

Access to Systems

You may have access to all or selected systems from the following based on your requirements and usage:

- HICL Network Access,
- HICL E-Mail,
- HICL Network Storage,
- HICL Core Business Application,
- HICL Human Resource Employee Self Service Portal & Management System, and
- Service Portals.

Authentication Mechanisms and Security Protocols

HICL has granted you access to its systems to enable you to achieve its objectives. You agree, to not knowingly permit use of your logon identification, password, workstation identification, user identification, file protection keys or production read/write keys, digital certificates, or 2-factor authentication mechanisms by any other person/entity and for the aforementioned mechanisms for any purpose other than what is required to perform authorized functions. You also agree that you will not disclose information concerning any access control mechanism (e.g., logon and password) unless authorized to do so by appropriate authority (being a member of the SMT or CEO). Further you will not use any access mechanism that HICL has not assigned to you.

You also agree to create or change your password when notified and to complete required information technology security awareness training annually as a condition of maintaining access to HICL systems. You will follow the security procedures of HICL computer systems as they are communicated and protect the data contained in them. You will not respond to phishing or other attempts to steal logons and passwords or introduce malware into HICL systems and will use care when opening attachments.

Data Confidentiality

You will treat all customers and personnel information maintained on the HICL computer systems as strictly confidential and will not release information to any unauthorized person.

File/Data Sharing Software

You will not use peer-to-peer file sharing programs such as BitTorrent, or similar programs on any HICL computer and will not download or share files in violation of that material's copyright protection.

Protection of Copyright

You are responsible for understanding how copyright law applies to electronic transactions. You should not violate the copyright protection of any information, software, or data with which you come into contact through the company's computing resources. Downloading or distributing copyrighted materials such as documents, movies, music, etc., without the permission of the rightful owner may be considered copyright infringement, which is illegal under copyright law. Use of the Company's network resources to commit acts of copyright infringement may be subject to prosecution and disciplinary action.

Adherence to Internal Policies, Procedures and Standards

You agree to abide by all applicable policies, procedures and standards that relate to the use of internet and electronic communication systems. These include, but are not limited to:

-
- Attempting to gain access to information owned by the HICL or by its authorized users without the permission of the owners of that information;
 - Accessing, downloading, printing, or storing information with sexually explicit content as prohibited by law or policy;
 - Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;
 - Installing or downloading computer software, programs, or executable files contrary to policy;
 - Uploading or downloading copyrighted materials or proprietary agency information contrary to policy;
 - Sending e-mail using another's identity, an assumed name, or anonymously;
 - Attempting to intercept or read messages not intended for them;
 - Intentionally developing or experimenting with malicious programs (viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.) on any HICL-owned computer;
 - Knowingly propagating malicious programs;
 - Changing administrator rights on any HICL-owned computer, or the equivalent on non-Microsoft Windows based systems;
 - Using HICL computing resources to support any commercial venture or for personal financial gain.

Reporting and Disclosure

If you observe any incidents of non-compliance with the terms of this agreement, you are responsible for reporting them to the management of my company.

Acceptable Use

You understand that you must use only those computer resources that you have the authority to use. You must not provide false or misleading information to gain access to computing resources. HICL may regard these actions as criminal acts and may treat them accordingly. You must not use HICL IT resources to gain unauthorized access to computing resources of other institutions, organizations, individuals, etc.

HICL reserve the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on HICL systems to ensure compliance with HICL policies, and federal, or local regulations. HICL or System Office officials will have the right to review and/or confiscate (as needed) any equipment connected to HICL owned device or network.

You also understand that HICL's IT Support Services reserve the right, without notice, to limit or restrict any individual's computer access and to inspect, remove, or otherwise alter any data, file, or system resource that may undermine any HICL information technology resources.

You hereby certify that you understand the preceding terms and provisions and that you accept the responsibility of adhering to them. You further acknowledge that should you violate this agreement; you will be subjected to disciplinary action.

Name _____ Code _____ Location _____

Signature _____ Date _____