



Cargo Handling Corporation Limited

Information Security Policies

[VERSION 2023A]

IT DEPARTMENT

Cargo Handling Corporation Limited

Last Updated July 2023

Approved by the Board of Directors of the Cargo Handling Corporation Ltd on 4 December 2025

Table of Contents

1. OBJECTIVE	1
2. INFORMATION SYSTEMS ARE FOR BUSINESS PURPOSES	1
3. MONITORING	1
4. DATA PROTECTION	1
5. DATA RETENTION POLICY	2
6. PROHIBITED ACTIVITY AND USE OF GOOD JUDGMENT	2
7. INTELLECTUAL PROPERTY AND LICENSING	3
8. VIRUS PROTECTION	3
9. PASSWORD PROTECTION POLICY	3
10. INTERNET USAGE	4
11. REMOTE ACCESS	6
12. CHANGE MANAGEMENT PROCEDURE	6
13. IT EQUIPMENT	6
14. DISCIPLINARY ACTION	7
15. RELATED LEGISLATIONS	7
USER AGREEMENT	8
ANNEXES	9

1. Objective

This document sets forth the policy of Cargo Handling Corporation with regard to the use of, access to, review, and disclosure of various electronic communications, including those sent or received by Company employees. This information systems policy applies to all individuals using the Company's computer and network systems, including employees, subcontractors, and consultants.

2. Information Systems are for Business Purposes

Information systems offered by the Company are provided to its users for the primary purpose of Company-related use.

Personal use is permissible on a limited basis. This limited personal use should not be during working time and should not interfere with job performance. Personal messages may not be broadcast to groups of people or employees. Permission for Company-wide broadcasting of personal messages must be obtained from your manager.

3. Monitoring

Electronic communications through the Company's information systems are the property of the Company to assist it in carrying out business. The Company treats all electronic communications sent, receive, or stored as business messages, including those for personal use. All users shall have no expectations of privacy with respect to any electronic message. While the Company will not do this routinely, it reserves the right to monitor, access, review, copy, store, or delete any electronic communications, including personal messages, from the system for any purpose and to disclose them to others, as it deems appropriate.

4. Data Protection

The CHCL also processes personal data that relate to employees and is therefore required by law to comply with the Mauritius Data Protection Act 2017 (DPA) <http://dataprotection.govmu.org/English/Legislation/Pages/Data-Protection-Act-2017-.aspx>, which protects the privacy of individual personal data and ensures that they are processed lawfully. Compliance with the DPA and its policy is the responsibility of all employees and everyone who has access to personal records. A breach of this policy, whether deliberate or through negligence could also lead to criminal prosecution. Employees handling personal data will be required to sign the CHCL Non-Disclosure Agreement.

5. Data Retention Policy

There is no general data retention law in Mauritius. There are, however, sector-specific record keeping requirements. For example, under Section 153 of The Income Tax Act 1995, records of employee emoluments must be kept for a period of at least five years. Under the Banking Act, a financial institution is required to keep a record for a period of at least seven years after the completion of the transactions to which it relates.

The CHCL will retain transactional data up to 10 years following which the data and messages may be cleaned.

Systems access, emails and other accounts will be deleted upon two consecutive years without usage and upon retirement of employees unless officially instructed otherwise by CHCL Management.

Employees' retirements and transfers will be as per official communication by the HR Department to the IT Department.

6. Prohibited Activity and Use of Good Judgment

Use of electronic communications to engage in any communication or action that is threatening, discriminatory (based on language that can be viewed as harassing others based on race, creed, color, age, sex, physical, handicap, sexual orientation, or otherwise), defamatory slanderous, obscene, or harassing is prohibited. Electronic communications shall not disclose personnel information without authorization. The destruction or alteration of electronic communications with the intent to cause harm or injury to the Company or an employee of the Company is strictly prohibited.

Electronic communications shall not be used for any illegal purposes or violate the intellectual property rights of others. Employees shall not break into the computers or intercept the communications of other individuals.

Employees will use the same good judgment to prepare electronic communications, as they would use in preparing a hard copy of a memorandum. The content of electronic communications may have significant business and financial consequences for individuals of the Company and may be inappropriately taken out of context. Because of the ease of sending these documents, extra care must be taken to ensure that they are not sent hastily. Please keep in mind that your messages may be read by someone other than the addressee. Accordingly, please ensure that your messages are courteous, professional, and business-like.

7. Intellectual Property and Licensing

The ease of copying through various electronic communications systems poses a serious risk of intellectual property infringement. Each user must be aware and respect the rights of others.

Software that may be marked as "free," "public domain," and "public use" may be free for personal use, but not corporate use. In downloading software from the Internet, use of this software can violate copyright or licensing requirements. Always obtain approval from the IT Department before using any publicly available software package.

Do not copy software licensed to the Company.

Users may not install software that originally came from your home computer or elsewhere unless you can demonstrate from a written license that such use is permitted.

Do not copy software owned by the company without appropriate permissions.

Do not remove intellectual property notices of others.

8. Virus Protection

Users may not knowingly create, execute, forward, or introduce any computer code designed to self-replicate, damage, or otherwise impede the performance of any computer's memory, storage, operating system, or software.

Software and other files may not be loaded on the Company's computers unless a virus check is performed using an approved virus-scanning program. It is a violation of this policy to disable any virus-checking facilities installed on any system or network.

9. Password Protection Policy

Access to CHCL systems is granted following approvals as per the CHCL Account Request Form at annex. Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members. All passwords are to be treated as sensitive and confidential CHCL information. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

All system-level passwords must be changed on at least a quarterly basis. All user-level passwords (Example Windows, HRMS, Financials, ...) must be changed at least every six months. The recommended change interval is every four months.

Users should be aware that monitoring of email and other user accounts provided by CHCL can occur if necessary.

10. Internet Usage

The CHCL's internal network is connected to the Internet. Everyone with computer and/or WIFI access to the internal network has the ability access the Internet, including use of electronic mail and the World Wide Web. While the Internet is a great resource for our organization, it is the responsibility of each employee to use this resource responsibly and respectfully. It is assumed that the predominant use of these resources will be for work use, and that any personal use of electronic mail or the World Wide Web will be limited; never a priority over work matters. If an employee is found spending excessive time on personal use of these resources, this privilege may be revoked for that employee.

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another department or changes job functions, a new Account Request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes;
- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information.
- Reference regulatory or technical information.
- Research

Personal Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action. Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

Approval

Internet access is requested by the user's manager submitting an Account Request Form to the IT department along with an attached copy of a signed Acknowledgment Form. Both forms must be approved by the employee's head of department.

11. Remote Access

For the purpose of data protection and data security, the CHCL do not provide employees with remote access to IT systems unless instructed otherwise by the CHCL Managing Director in exceptional situations (e.g. COVID 19 lockdown, Overseas travel).

Remote access is used for urgent business-critical technical intervention by IT Administrators and contractors only.

12. Change Management Procedure

Any request for change in existing applications, parameters or data must be made officially using the Change Request Form annexed.

13. IT Equipment

Installation, movement, replacement, damage reporting and disposal of IT equipment must be made through IT Staffs only. Find annexed required Asset Replacement and Damage Reporting Form.

Disposal of IT equipment is allowed only following verification and approval of the Internal Audit Department.

Read the CHCL ***IT Equipment Usage Guidelines and Policies*** for more detailed guidelines on CHCL IT equipment provided for official use.

14. Disciplinary Action

Management reserves the right to revoke any user's access privileges at any time for violations of this policy and conduct that disrupts the normal operation of the company's information systems. Any conduct that adversely affects the ability of others to use the company's systems and networks, or which can harm or offend others, will not be permitted. Violations to this policy can result in termination.

Authority may be exercised without notice and management disclaims responsibility for loss or damage to data and software as a result.

15. Related Legislations

[Computer Misuse and Cybercrime Act 2003](#)

[Data Protection Act 2017](#)

[Electronic Transactions Act 2000](#)

[Information and Communication Technologies Act 2001](#)

[The Cybersecurity and Cybercrime Act 2021 \(Proclaimed on 10 December 2021\)](#)

[The Electronic Transaction Act 2000](#)

User Agreement

I have read and I understand the Cargo Handling Corporation Ltd Information Security Policies version 2023A and its related contents. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

Name: _____

Grade: _____

Department: _____

Location: _____

Signature: _____

Date: _____

Annexes

Cargo Handling Corporation Limited

Information Technology Department

ACCOUNT REQUEST FORM

Action Requested

Delete Account ☐

Modify Account ☐

New Account ☐

User Information

User Name: _____ Emp Code: _____

Grade/Dept: _____

Location: _____
(Head Office, MCT, MCT Yard, MPT, etc)

Application: Windows ☐ HRMS ☐
Email ☐ ERP ☐
XPS ☐
N4 OPS ☐
N4 Billing ☐

Other (specify):

Approval Information

Approved by (HoD): _____ Position Held: _____

Signature: _____ Date: ____/____/____

M.D. Signature: _____ Date: ____/____/____

IT Department Only

User ID(s): _____ Created/Modified/Deleted by: _____

Signature: _____ Date ____/____/____

IMPORTANT: Users are responsible for all activities under their login ID and the IT department do not record any password. Please refer to the IT Security and Internet Access Policy document for more details.

CARGO HANDLING CORPORATION LIMITED
REPLACEMENT OF FIXED ASSETS FORM

SECTION A : REQUEST FOR REPLACEMENT OF FIXED ASSETS

This Section must be filled by User/Dept. making request for new fixed assets.

ASSETS TO BE REPLACED:.....

MAKE & MODEL:.....LOCATION:.....

USER(S):.....POSITION HELD:.....

REASON(S) FOR REPLACEMENT:.....

.....

.....

APPROVAL OF HEAD OF DEPARTMENT: DATE:.....

SECTION B: RECOMMENDATION FOR REPLACEMENT

This Section must be filled by IT Department. (Where Applicable)

ASSETS VERIFIED BY:.....POSITION HELD:.....DATE:.....

RECOMMENDATION OF IT MANAGER:.....

.....

.....

SIGNATURE:.....DATE:.....

SECTION C: REPLACING ASSET

This Section must be filled by Purchasing Section.

DESCRIPTION OF ASSET PURCHASED

ASSET TYPE:.....MAKE & MODEL:.....

DATE OF PURCHASE:.....COST:.....SUPPLIER:.....

SIGNATURE OF PURCHASING OFFICER:.....DATE:.....

DELIVERED TO:.....POSITION HELD:.....

SIGNATURE:.....DATE:.....

Cargo Handling Corporation Limited

Information Technology Department

IT Equipment Damage Report Form

IT Equipment

RDT ☐

PC/Peripherals ☐

Printer/Scanner/IP Phone ☐

Damage Reported

Reported by: _____

Code: _____

Grade/Dept/Team: _____

Location: _____

Previous User/Team: _____

Description: _____

Signature: _____

Date/Time: _____

HoD Signature: _____

Date/Time: _____

Action Taken (IT Department)

ITM Signature: _____

Date/Time: _____

Cargo Handling Corporation Limited

Information Technology Department

Change Request Form

[illegible]