Anchor Group IT Charter

Preamble

Computer security in the Group is a shared objective that can only be achieved in an atmosphere of loyalty and mutual trust. The purpose of this Information Technology (IT) Charter is to define the rules concerning the use of computers and other IT systems at Anchor Group.

The constant progress of information processing and communication techniques has increased the need to specify the rules required to protect the privacy of Anchor Group employees, while also maintaining the prerogatives of system administrators and security.

This Charter is applicable to all Anchor Group IT services users.

Introduction

The rapid development of IT and digital networks within firms and throughout the world constitutes an extraordinary collective wealth but has also revealed threats of abuse as well as weaknesses which cannot be ignored. There are many potential IT-related risks and compliance with these rules is the inevitable price to pay for freedom in communication and use of company computer systems.

The user shall therefore be held personally liable for failure to comply with the IT Charter of Anchor Group, which may directly or indirectly impair all or part of the company's operations. The company is itself subject to rules governing the proper use of computer systems and must therefore uphold both the code of good practice and all legislative requirements. Security will only be achieved through vigilance and if all employees abide by the rules.

Scope of application

The rules and obligations set forth below apply to any person, regardless of his or her status, authorised to use the Anchor Group's computer and network facilities. Here, facilities shall *inter alia* include computer systems or servers, workstations, terminals, portable drives, mobile computer equipment, phones, tablets, printers, scanners and all related hardware and/ or software.

Compliance with the rules as defined by the IT Charter also applies to the use of computer systems of independent organisations as well as systems that can be accessed by telephone, digital networks and cloud-based technologies and applications.

Rules of good practice

1. Anchor Group's IT Charter is a set of good practice rules to which employees and users must comply. The Charter aims to inform and warn users of the risks involved in using the Group's IT infrastructure and network.
2. The Group's IT systems are to be used exclusively for the performance of professional tasks for which they are designed. Consequently, any file or email stored or transferred via the Group's IT system/ network is deemed to be of an exclusively professional nature and, as such, cannot be considered private.
3. Point 2 above excludes those instances where prior authorisation is granted by the manager/s concerned, these systems may not be used to carry out projects that are not part of tasks or responsibilities entrusted to users and related to the day-to-day operations of Anchor Group.
4. Using the Group's IT systems for personal purposes is inevitable. However, users must familiarise themselves with the various IT protocols to ensure compliance with this Charter.
5. Participation in games on the company network, non-professional data exchanges and other recreational or personal financial applications are strictly prohibited.
6. Data conveyed or saved on the network by users must be both legal and lawful. Therefore, users must abide by all legal provisions.
7. Each user agrees to take care of the hardware provided to him/ her and to inform the IT Department of any anomaly noticed.
8. In the event of a user's foreseeable absence equal to or longer than half a day, each user agrees to activate the automatic absence-messaging function beforehand.
9. In the event of an unforeseeable absence equal to or longer than half a day, the relevant employee's line manager reserves the right to ask the IT Department to activate this automated message and/or the redirect all of the user's messages to another mailbox.
10. Each user agrees to store, in a place shared by the relevant employees of the Group, those messages or files required for their job to be continued in the event of their absence. Otherwise, in the event of an absence equal to or longer than half a day and in the event of an urgent business need, the relevant employee's line manager reserves the right to ask the IT Department to give temporary access to another user so that he/ she may retrieve the messages or files needed to ensure business continuity.
11. Activities that might take up a lot of computer space (printing large documents, substantial calculations, intensive use of the network or mailbox etc.) must be carried out at times that cause the least amount of disturbance to the rest of the community of users/ employees.

Each user, by logging on, agrees not to:

1. intentionally carry out, attempt to carry out or cause to be carried out any operations intended to harm a person, the Group or any other establishment;

2. intentionally change or destroy information on one of the systems connected to the network;
3. intentionally interrupt the normal operation of the network or of one of the systems connected to the network;
4. connect or attempt to connect to a protected site without prior authorisation;
5. attempt to read, copy or disclose data protected by another user;
6. change another user's data without having explicit authorisation to do so;
7. conceal their true identity;
8. appropriate another user's password;
9. spoof machine names, addresses, or identities;
10. intercept, or attempt to intercept, communications between third parties;
11. connect peripherals or computers such as computer storage units or personal laptops to the Anchor Group internal network without prior authorisation from the IT Department.

Responsibilities

System administrators

1. Anchor Group's systems and networks are managed by system administrators that are responsible for the proper operation thereof and the quality of the service provided within the limits of the means allocated.
2. Despite regular backups, the restoring of files is not guaranteed even if the system's administrators do their utmost to retrieve lost files.

Duties

In accordance with the means at their disposal, system administrators are required, above all:

1. to enforce the rights and responsibilities of users;
2. to respect, when they are themselves users of computer systems, the rules that they impose on other users;
3. to inform their superiors of any non-compliance with the IT Charter;
4. to respect and uphold the confidentiality of files, emails and any data under their responsibility;
5. to ensure security and confidentiality of the networks by using all technical and human resources required;
6. to inform users, as far as possible, by all appropriate means, of any intervention likely to disrupt or interrupt the ordinary use of the firm's computer facilities;
7. to keep interruptions in computer services to a minimum and to choose dates and times that are the least detrimental to network users;

8. to cooperate with the security agents of independent networks in the event of a security incident/ breach involving a network which they administrate.

Rights

To mitigate a possible incident in operation or security, the system administrators may:

1. take conservatory measures;
2. stop the execution of any IT process or service;
3. remove rights of access and/ or passwords;
4. close a network to the outside world;
5. stop any server.

The need to act, as an exception, on the services, data and communications must be justified by an urgent collective need assessed by the superiors or, in an emergency, directly by the system administrators.

Accounts and passwords

1. The network accounts are created and closed by the IT Department. These accounts are temporary, strictly personal and non-transferable. They shall be terminated when the account holder leaves the employment of Anchor Group.
2. A new user's access ID is granted once he/ she has been informed of the existence of the IT Charter.
3. The system administrators may, with or without giving notice, take the necessary steps against any user (including temporarily closing his or her account) who disrupts the smooth operation of the computer facilities or who fails to comply with the rules set out in this document. The user may contact the manager responsible for the IT Department or Anchor management, which may take the appropriate actions to resolve the problem.
4. Passwords may not be disclosed to any third person, including system administrators. Right of access may be transferred, if needed, to another user for service-related reasons after notification by the system administrators to the manager/s concerned. As a general rule, the manager (or a person appointed by him/ her) is responsible for informing system administrators of any changes concerning the right of access of a user e.g. the temporary transfer of the right of access (absence, leave, etc.), change of function leading to a change in the right of access, change in the civil status at the user's request, removal of an account etc.
5. All passwords must respect the requirements of complexity and length which are defined by the IT Manager (*see the Password Protocol*).

Each user agrees to:

1. contribute to security on a personal level; each user is responsible for the computer operations, both local and remote, conducted using his or her account;
2. take the necessary steps, in the event of absence, to make the data under his or her responsibility accessible to the company;
3. immediately inform the system administrators if his/ her password no longer allows the user to connect, or if the user suspects attempted or actual piracy of their account.

Security

The user must take the necessary precautions to:

1. keep his/ her password secret;
2. protect his/ her files;
3. normally end his/ her sessions of connections to the company's computer facilities;
4. lock access or disconnect his/ her workstation from the network;
5. keep in a secured place any digital media which might contain confidential, professional or personal data;
6. to protect data that guarantees compliance with the confidentiality undertakings made by the company to third parties.

Each user agrees

1. that the cryptography, to ensure the confidentiality of data, may not be used to conceal information that breaks the code of good practice established by the IT Charter;
2. not to introduce viruses intentionally and to strive to avoid the spread of any viruses through the firm's IT systems,
3. to ensure the security of the IT systems, the IT Department must be informed in case of doubt concerning the transmission, the content of a message or an appended file. The IT Department must be immediately informed if a virus is detected or an anomaly noticed in a mail or an appended file. When a virus is detected, such e-mail must not be opened by the recipient but immediately destroyed (*see the Phishing Protocol)*;
4. not to do any research into the security of the firm's IT systems without prior authorisation from the system administrators;
5. not to download, develop, install or copy a software tool to circumvent security, saturate facilities, illegally open a communication port, circumvent software protection, decrypt passwords, pick up information on the network etc.;
6. not to make use of any holes in security or anomalies in operation;
7. to inform the system administrators of any holes in security and to refrain from advertising such information.

Privacy and personal data

Users are advised that system administrators, as part of their work;

1. have specific rights to access any stored or circulating documents on the Anchor Group networks. Users agree to only use the network for the proper operation of the computer facilities according to the terms stipulated herein;
2. may keep a history of all connections to the network, access to the Internet, messages sent and received, access to databases and changes to data in the event of a security problem or system malfunction;
3. may archive these journals (log files) for a maximum term of 3 months. They are not examined unless there is an absolute necessity to do so for security reasons or due to system operations. The decision to examine such information may be made as part of a legal enquiry,
4. may keep a history of the nominative data for a maximum term of 3 months. They may be consulted only when required by law or for history purposes;
5. may monitor work sessions in progress if they suspect failure to comply with the IT Charter or in case of technical problem;
6. may compress or move, with or without giving notice, any files considered to be excessive in size or delete, after giving notice, with the owner's agreement or decision from the Manager;
7. may move, with or without giving notice, any files without a direct link to the professional use of the computer system or delete, after giving notice, with the owner's agreement or decision from the Manager;
8. reserve the right to change the priority of a task or to stop the execution thereof in the event of abusive use of the network facilities, after notifying the user concerned, if possible.

Users are informed that:

1. data processing of personal information shall be conducted in full compliance with the provisions of the law;
2. the right of privacy of each person shall be respected;
3. the publication of personal photographs on the public domain (Internet) requires the express consent of the person involved;
4. the possibility of reading a file does not grant authorisation to read it;
5. general laws prohibit the following types of information or messages: Insulting or abusive language and imagery that portrays pornographic, paedophiliac, slanderous, incitement to racism or xenophobia, any attack on human dignity etc. (*see the Social media protocol*).

Software and copyright

Users must not under any circumstances:

1. download, install or copy any software to Anchor Group computers or network, including software that is part of the public domain or make such software accessible on the network, without obtaining explicit prior authorisation from the IT Department;
2. duplicate protected software;
3. copy an application developed by the Anchor Group without prior authorisation;
4. export all, or part, of the source codes of applications outside the Anchor Group buildings;
5. circumvent the restrictions of software use.

Sanctions

Any user failing to comply with the rules and obligations as set out in this IT Charter is subject to disciplinary actions provided for in the Anchor Group Human Resources Manual.