Code of Conduct for Digital Protection DS_GC01

OWNER: L. THOMAZEAU REFERENCE: DS_GC01

Main recipients: All employees

Revision	Issue date	Prepared by	Approved by	Changes
0	04/2005	S. AUBERT	J.P. GAGNEPAIN	
1	02/2015	Y. PIEDERRIERE	F. ABRIAL J.P. GAGNEPAIN L. DUBLANCHET	
2	08/2019	GIO/EUS GDSD	F. GAUDRE L. THOMAZEAU	

Table of contents

Executive Summary

Welcome to the Code of Conduct for Digital Protection at Air Liquide.

This Code is a key part of the Group Digital Security Policy (**DS_GP00**) in the BlueBook. **It concerns all employees**, whatever their position or seniority, as well as authorized personnel from third parties (such as consultants, contractors) under service contract with Air Liquide. It specifies the **User's duties and responsibilities** in ensuring the proper use and **protection of Air Liquide's digital resources and information.**

It constitutes a document of reference for all the entities belonging to the Air Liquide Group, and forms part of the internal regulations. It applies to all Digital Resources as defined in the Glossary, including data and information in all forms, digital or paper.

The Code does not aim to exhaustively describe all possible situations, but sets out general principles for use. It is therefore intended that each User (as defined in the Glossary) will act in accordance with these principles when faced with unforeseen situations. The Code may evolve in response to the legislative context and the Group's internal regulations. Additional rules may be communicated by any of the Group's entities specific to their own context or requirements, either regulatory or internal. **The requirements in this Code do not supersede any stricter local legislation.**

1. Purpose

Why the Code?

Every part of the Group's operations, activities and know-how inherently depends on digital systems interconnected in an increasingly open and mobile ecosystem of relationships and information flows both internal and external.

With the numerous opportunities to improve the way we work, operate and collaborate, this dependency also brings new and increased digital risks which may result in a breach of sensitive information or the compromise of digital systems, affecting the Group's reputation, financial situation or people and operations integrity.

Potential threats are growing in number, diversity and complexity. They include negligence and errors, malicious acts such as intrusion, cyber-attacks, cyber-espionage, malware, fraud, etc., and accidents and natural disasters such as fires, floods, etc. All of these could disrupt access to and availability of digital resources which are vital for Air Liquide's daily operations. Other potential consequences include the breach of confidential information, destruction or corruption of data, or damage to the company's reputation.

This Code defines the **key principles and rules to be followed by Users when accessing or using Air Liquide's digital resources and information**.

Every User must comply with the legal, regulatory and contractual requirements in terms of digital conduct and data protection, which are increasingly specific, both at the national and international level, wherever the Group operates.

Protecting information and Digital Resources is everyone's responsibility.

It is the responsibility of each User to read and apply this Code. It is available, together with Group Digital Security Policy (**DS_GP00**), on the BlueBook intranet under the heading "Digital Security".

For any additional information about the Code, or about digital security and information protection procedures, ask your supervisor or check with the **Information Protection Coordinator of your Entity**. We thank you for your vigilance and for your role in ensuring a safe, reliable and productive work environment.

2. Key Principles

Note: terms with capital letters are defined in the glossary in the appendix of this document.

::: 1 Public digital communication networks – including the Internet or mobile network – and private systems and networks such as Air Liquide's **are not lawless zones**. The User must perform his or her activities in compliance with all applicable legislation and regulations, including the rules of the Group (such as those outlined in this Code) and any instructions specific to the User's particular entity.

::: 2 Access to Digital Resources and communication networks is provided to the User **for the conduct of his or her professional activities**:

- You are responsible for applying any updates asked by the IT teams to maintain the level of security at the right level.
- You are responsible to keep your credentials safe. You can be held responsible for the actions done with your credentials if you communicate it to someone or don't protect it.
- This usage must be honest and reasonable so as not to disrupt operations and to avoid such resources from being diverted toward illicit or non-professional ends.
- Everyone must contribute to the general security of the Group.

::: 3 **Personal use** cannot in any case be considered as a right, but as something that is tolerated by the Group. It must remain reasonable and occasional, and must not affect working operations, the protection of data, the security of Digital Resources, or the Group's interests. **User's private data must be clearly labeled as such**.

::: 4 The User must not transmit confidential information, nor make it available or offer it to non authorized individuals.

::: 5 If, in the performance of his or her duties, an employee needs to create or handle data files containing legally regulated information (e.g. personally identifiable information, export control...) he or she must ensure beforehand that such files as well as their use conform to legislation currently in force.

2.1. Digital systems and the laws

::: 6 Every individual who uses Air Liquide's Digital Resources must comply with the laws relating to the use of such systems and the transmission of information. The laws and regulations generally include provisions forbidding:

- **Violation of privacy** (subjects relative to, among other things, political, philosophical or religious opinions, ethnic origins, sexual orientation, or health);
- Acts of written or verbal violence or **acts contrary to ethical rules** (in particular slander and abuse; inciting crime and offences and inciting suicide, inciting discrimination, hate - particularly racial -, or violence; revisionism and apology for crimes, in particular murder, rape, war crimes and crimes against humanity; compromising children or exposing them to violent or pornographic material; inciting the consumption of prohibited substances);
- **Computer fraud**, which includes such things as:
  - Fraudulent access to and/or remaining connected to an information system;
  - Falsifying, modifying, deleting or adding information with the intention to harm;
  - Modifying, deleting or adding processing commands on a system for the purpose of falsifying or otherwise corrupting its performance;
- **Violation of business secrets** (disclosure of Confidential Information, commercially sensitive information, etc.);
- Acts in breach of the rules protecting **intellectual property rights**, in particular: trademark counterfeiting and copies of commercial software for any purpose whatsoever and breach of copyright;
- Breach of regulations concerning files containing **personally identifiable information**; in particular sensitive information like patient data.

If you have any questions or concerns, you should always ask your manager or legal department.

3. User Access

The User identifier (User id or login) and associated authentication code (password, second factor for authentication) are the fundamental elements to access and use information and Digital Resources. They are unique to the employee and uniquely engage the employee's responsibility.

The management of each Entity is responsible for the **proper allocation, maintenance and revocation of User accounts and access rights** (log-in identifiers and passwords) of its personnel. Access rights shall

be terminated in a timely manner from the moment that the mission or professional activity which justified it comes to an end.

::: 7 Means of authentication including passwords and/or Security Tokens (see glossary) are **strictly individual and must be kept confidential** at all times by the employee.

::: 8 The User must only access information or resources to which he or she has legitimate or authorized access to. If a User considers that their level of authorization is inadequate with respect to their mission, he/she should ask their supervisor to modify their access rights accordingly.

::: 9 The User must under no circumstance attempt to access, by covert or improper means information or digital resources to which they have no legitimate or authorized access; this includes and is not limited to circumventing access control mechanisms, impersonating another employee, using the access credentials of another User.

4. End-User Devices

4.1. Working with Devices provided by Air Liquide

It is the policy of Air Liquide to provide employees with the devices and tools needed to perform their work.

::: 10 Each User must follow the rules in force concerning the configuration and use of his or her devices provided by Air Liquide (PC, smartphone, tablet...):

- **Users shall take due care of equipment** provided by Air Liquide, and in particular take every precaution to prevent the device(s) from being stolen.
- **Users must not circumvent the device's security**. The User must keep it such as it was configured by the IT services, in particular with regard to operating system configuration, antimalware, encryption, password policy and other security parameters.
- Users must follow the procedures indicated by the IT services for connecting devices to the Group's Digital Resources and the Internet.
- Users shall keep the devices up-to-date with software levels and apply updates regularly once notified by the system. In the case of laptops, the User must connect periodically to the company's network so as to ensure that antimalware protection and other security updates are applied.
- Removable storage media (USB keys, hard drive, memory cards...) can be infected by malware, and could be lost containing sensitive information. For these reasons, their usage must be avoided whenever possible, and **limited to storage media of trustworthy origin and with encrypted content.**

::: 11 The User must protect the integrity and availability of all information for which he or she is responsible. In particular the User must regularly make backup copies, using tools recommended or provided by the IT services, with a level of frequency and protection appropriate for the risk of loss of the information.

::: 12 The User must comply with any communicated software terms of usage and restrictions, including when using "Cloud" applications and services.

::: 13 Users must never download, install or use additional software and applications on Air Liquide's workstations, unless these have been provided or authorized by the local IT Services.

4.2. Working with Private Devices

Air Liquide tolerates for Users the possibility to use Private Device(s) (smartphone, tablet) for work-related purposes (so-called "mixed usage"). However, using such device(s) won't allow access to Confidential information and/or Critical Digital Assets. This is done in the spirit of giving employees the **flexibility** to use the devices which are most familiar and effective for them. This possibility is **strictly governed by the key principles and ground rules** below.

::: 14 "Private Device" in this Code specifically and exclusively designates the User's own device whether the User's own property or for which the **User takes full accountability** with respect to the use, integrity and security of the device.

::: 15 The use of **public** devices (e.g. in cybercafé, kiosk or other self service devices) to access Air Liquide Digital Resources or to handle Air Liquide Sensitive Information is **strictly prohibited**.

::: 16 The use of Private Devices for company-related work is strictly the sole choice and responsibility of the User. The User accepts that such use does not amend in any way his/her rights and obligations as an employee.

::: 17 The User will act and behave in a trustworthy and responsible manner as when using company-provided devices, and in particular **will comply with the rules as detailed in th**e User Agreement for Secure Use of Private Devices (**DS_GP10**).

5. Digital Workplace

The Group provides Users with a worldwide digital platform (the digital workplace) for the conduct of their professional work and activities for Air Liquide. This digital workplace is a comprehensive suite of personal and collective tools to create, communicate, share and collaborate easily and fluidly; it includes office tools, email, instant messaging (chat), document sharing with collaborative working functionalities, audio and video meeting, etc...).

::: 18 The digital workplace is the common platform of the Group for Users to do their work. Users should not use tools which are not part of the digital workplace in the conduct of their work unless those tools have been expressly approved by the Group.

::: 19 **The User has the responsibility to protect sensitive information**, i.e. both legally regulated and company confidential information according to the rules of the Group Confidential Information Protection Procedure (**DS_GP02**).

- In particular, ●●●CONFIDENTIAL-SECRET and sensitive personally identifiable information shall be handled only in compliance with applicable laws and with appropriate tools and systems approved by the Group, such as the *Digital Guard* tool.

::: 20 Users must be careful when sharing information (documents, emails, orally...), in particular with third parties external to the Group.

6. Internet and Social Media

Users should be mindful that surfing the Internet leaves traces on the sites visited (including IP address, previous pages visited, earlier contributions to forums, etc).

Using the Internet also exposes computers, Users, and therefore Air Liquide, to many risks, such as hijacking of the Group image, viruses, etc.

::: 21 Connections are authorized to sites relating to the User's professional activities and care must be taken to respect the specific rules of sites visited, as well as those applying to the Group and/or each entity.
A reasonable and occasional private use is tolerated.

::: 22 The User must not communicate sensitive information relating to Air Liquide (whether personal, confidential, or jeopardizing the Group's image, for example) without prior authorization, in particular in forums, online chat rooms and other document sharing platforms.

::: 23 As part of his/her private life and in particular on all social media, when the User has to disclose its relationship with the Group or refers to the Group, he or she must comply with the duty of loyalty and discretion; as per the Group's Code of Conduct Key Concepts (CSR_GC02) and Use of public social media by Air Liquide employees (COM GC01) requirements (see Bluebook).

::: 24 Users shall not use their Air Liquide's professional identifiers (e.g. emails...) for private activities (online services, web sites registration...).

7. Security Incidents

Our ability to continually detect and treat security incidents is a crucial component of our digital protection system. It provides the vital sense and respond capability to **keep us constantly on the alert** and be **prepared to respond** to cyber-threats, vulnerabilities and any anomalous situations developing in our environment.

::: 25 Every User has the responsibility to immediately report any anomaly or suspected security breach to the Helpdesk or the local IT manager as per Bluebook "Digital Security Incident Management Procedure").

8. Monitoring and Sanctions

The rules and guidelines contained in this Code are vital to the protection of information and for the proper use of the Group's Digital Resources.

::: 26 Air Liquide reserves the right to analyze, monitor and control the use of relevant resources and software as well as the exchanges, whatever their nature or object, transmitted across the Group's Digital Resources. In particular, Air Liquide puts in place filtering mechanisms blocking access to unauthorized websites and content.

::: 27 The checks will concentrate on the log files and will not be done in a systematic individualized manner, except where there is an anomaly. According to the relevant applicable procedure, the administrator will inform the User of the anomaly. These operations will be undertaken:

- With the objective of guaranteeing the correct operation of the Information System, its security and the interests of the Group;
- In accordance with applicable law;
- Exclusively under the responsibility of information technology services professionals who will maintain the confidentiality of information they may discover in the course of these operations in cases described in section 28 hereunder.

::: 28 In the event of serious circumstances of illicit use, or sensitive information leakage, or endangering the correct operation of the Digital Resources, their security or Group interests, IT service staff may do the following:

- Suppress or destroy the offending elements or those at risk of damaging the integrity of the system;
- Bring it to the attention of senior management.

::: 29 A log of connections and analysis will be kept for a period not exceeding twelve months except where another period is required by local legislation.

::: 30 In the event of a proven violation of this Code, Air Liquide may take disciplinary action corresponding to the seriousness of the problem, in accordance with internal company regulations and applicable laws and regulations.

::: 31 In the case of failure to comply with the applicable laws and regulations, Users will be held responsible for their actions and may be subject to the penalties (civil or criminal) provided for by law.

Glossary

Group: All entities under Air Liquide's operational control around the world.

Availability: Ensuring that authorized Users have access to information and associated assets when required. Also, the capacity of a system to fulfill a task according to the conditions defined by time and performance.

Integrity: Safeguarding the accuracy and completeness of information and processing methods. When information is exchanged, integrity extends to the authentication of the message (the guarantee of its origin and destination).

Confidentiality: Ensuring that information is accessible only to those authorized to have access.

Information: Information can include facts, data or opinion, whether written, digital, graphic or narrative, and maintained in whatever medium, including but not limited to paper, computerized databases or hardware supports.

Sensitive Information (or Confidential Information): Information of which inappropriate handling and/or leakage could adversely affect Air Liquide interests (e.g. ●●CONFIDENTIAL-RESTRICTED, ●●●CONFIDENTIAL-SECRET as per Bluebook "DS_GP02 Confidential Information Procedure") or the privacy to which individuals are entitled as per international/local personal information protection regulations (e.g. patient data, human resources information, social security number...).

Digital Resources is the generic term used to designate all information technology systems, services and communication networks (data, telephony), both public and private, which are used or accessible to Users in the conduct of Air Liquide activities and operations.

These Digital Resources include hardware equipment - PCs, terminals and access devices, servers, network components, firewalls and other security devices, etc... - software systems (operating systems, business applications, database systems, etc...) and IT services of all types, including management and support services such as access management and authentication, patch management, IT support, monitoring services, ...) and cloud computing services, such as SaaS applications (or Software as a service), computing capacity and platforms, on-line storage, etc… directly available on the public internet through subscription-based contracts. Digital Resources also includes by extension data and information which are contained, stored, carried or transmitted in the above "container" resources. Because of their particular value and importance data or information may be referred to as such specifically whenever Appropriate.

Digital Workplace: The digital Workplace is a comprehensive suite of personal and collective tools to create, communicate, share and collaborate easily and fluidly; it includes office software, email, instant messaging (chat), document sharing with collaborative working functionalities, audio and video meeting, etc…

Digital Information Safe is a highly secured system used to store, communicate and share the most sensitive documents of the Group (labeled ●●●CONFIDENTIAL-SECRET).

User: Designates individually all persons, whatever their level in the hierarchy, as well as third parties carrying out work orders for the company, having access to Digital Resources of the Group and/or to any information or data of Air Liquide.

Security Token: A security token (or sometimes a hardware token, authentication token, USB token, cryptographic token, software token, or virtual token) may be a physical device or software that an authorized User of computer services is given to ease and reinforce authentication.

Phishing: Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by pretending to be a trustworthy entity in an electronic communication like an email.

Cloud: Cloud computing is internet-based computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Clouds can be classified as public, private or hybrid (mixed).

Mobile device management (MDM) is an IT term for the technical administration of mobile devices, such as smartphones, tablets and laptops when linked to a corporate digital workplace. By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and business risks.

Private Device specifically and exclusively designates the User's own device or for which the user takes full accountability with respect to the use, integrity and security.

Containerization Solution: is a software solution that creates separate encrypted containers on a Private Devices to clearly delimit the corporate versus the private information and usages.

IT Services: internal departments in charge of the Digital Resources, both at Group Level, and locally.