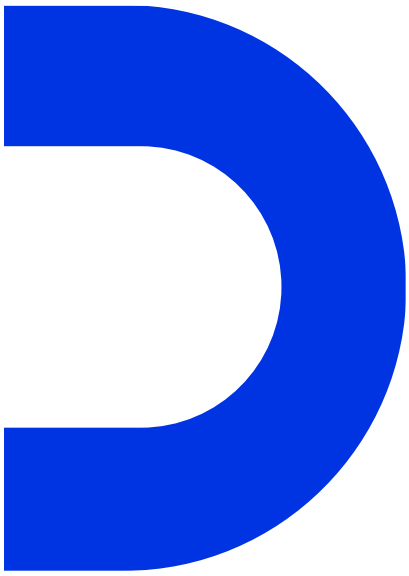

CONFIDENTIALITY, USE OF IT AND ASSIGNED ASSETS

Internal Regulations – Corporate Policies

Date: November 2021

Code: PC-04-5.2-09-202111

Introduction

Approval of the Global Dominion Access, S.A., (hereinafter "**Dominion**") Confidentiality, Use of IT and Assigned Assets Policy (hereinafter, the "Policy") is yet another milestone in Dominion's steadfast commitment to lawfulness, ethics and professionalism that underpins how it conducts its operations and its corporate culture.

Pursuant to this Policy, Dominion is firmly committed to:

- Complying with and fully adhering to all current legislation (both nationally and in the countries where it operates).
- Complying with the principles that govern its Code of Conduct which forms the basis of the Policy set out here.
- Training and raising awareness of the Obligated Parties (as this term is defined below), as well as stakeholders, of the importance of complying with this Policy and third parties engaging with Dominion.
- Applying penalties for non-compliance with the provisions set out herein, pursuant to the applicable disciplinary measures.

With this Policy, Dominion intends to establish the principles under which each of the employees, managers and administrators of all the companies that make up Dominion must process the information created or that they have access to within the scope of their professional duties at Dominion, protecting this information and preventing its unauthorised disclosure to third parties. The Policy also serves to set out the general guidelines with regards to computer and communication equipment, programmes, all types of software and hardware provided for professional duties to be carried out, and any other assigned assets.

This policy is closely related to the Privacy Policy for the Protection of Personal Data.

Scope of application

The Policy applies to all employees, managers and directors of all the companies that make up Dominion (hereinafter "**Obligated Parties**").

For the purposes of this Policy, "Dominion" shall also mean all companies which Global Dominion Access, S.A. controls or may control, directly or indirectly, with control being understood to be:

(i) holding the majority of the voting rights;

(ii) the right to appoint or remove a majority of members of the Board of Directors; or

(iii) holding the majority of the voting rights pursuant to eventual agreements made with third parties.

Likewise, all third parties who have dealings with Dominion will also indirectly receive this document and, whenever possible, must be made aware of the underlying principles and values.

Privacy and Protection of Information

Confidential Information

The following will be deemed to be **Confidential Information**:

- Any internal information that is specifically declared to be confidential and any third-party information that is submitted to or can be accessed by Dominion subject to confidentiality agreements.
- Information concerning Dominion's employees, managers or directors, Dominion's customers, its suppliers and other third parties, both physical or legal, associated with Dominion that has not been publicly disclosed by them or is not in the public domain.
- Documentation related to the activities performed by the various areas of Dominion that has not been publicly disclosed by them or is not in the public domain.

The obligation for discretion, secrecy and confidentiality

Disclosure of Confidential Information whether intentionally or by mistake, can seriously affect Dominion and/or its stakeholders and third parties. Accordingly, to ensure that such information is used with the required level of secrecy and confidentiality, the following obligations and principles of conduct have been established:

- Obligated Parties shall comply with the obligations regarding discretion, secrecy and confidentiality in relation to the Confidential Information they possess or which they have access to in order to carry out the tasks inherent to their job or the responsibilities entrusted to them by Dominion.
- The information shall be used for legitimate purposes and in an honest and responsible manner, and, in the case of information relating to identified or identifiable natural persons, it shall be used in full compliance with the provisions of any applicable data protection legislation.
- No Obligated Party may disclose Confidential Information either during or after the termination of their professional relationship with Dominion, without the necessary authorisation from Dominion.
- All Obligated Parties must immediately report to the person in charge of their department, area or unit in relation to the following:
    - Any use, disclosure and/or publication of Confidential Information by other Obligated Parties.
    - Any attempt made by a third party not associated with Dominion to obtain Confidential Information from any Obligated Party.

The Risk & Compliance department will be consulted whenever any doubts arise.

Mechanisms established to guarantee confidentiality.

The following basic measures must be implemented, to guarantee Confidential Information protection, as appropriate:

- Obligated Party acceptance of Dominion's Code of Conduct, which establishes specific requirements concerning the integrity and confidentiality of the information.
- The inclusion of a confidentiality clause in contracts Dominion enters into with third parties that involves dealing with Confidential Information.
- A confidentiality document signed by contractors, subcontractors, consultants and other third party suppliers of goods or services who have access to Confidential Information.
- Profile-based restricted access to Confidential Information on Dominion's internal network.

Personal data protection

In line with the access Obligated Parties have (based on their professional activity) to personal data that Dominion is in charge of processing, the former are bound to keep said data completely confidential, and to adhere to the provisions of both internal and external regulations relating to this matter.

Use of information and communication technology

General Principle

Any kind of IT and communication resources which Dominion provides to the Obligated Parties are exclusively intended to be used as work tools to carry out the professional functions entrusted to these parties. Accordingly, as a general rule, these resources cannot be used for private purposes or for purposes which are not in Dominion's interests.

Obligated Parties must not alter the configuration of their equipment, nor add or remove software, hardware or items relating to it, except for those parties who are specifically dedicated to doing so because of their functions.

The Parties must use all equipment assigned to them in a diligent manner.

Safety Measures

Obligated Parties are obliged to:

- Meet the safety procedures established to protect information and help safeguard its confidentiality.
- Protect all IT Systems that have been physically assigned to them, such as personal equipment, services, etc.

- Use all assigned equipment in a diligent manner.
- Never directly or indirectly disclose confidential information to anyone, except Dominion staff or its suppliers who need such information to carry out the roles they have been assigned.
- Only process information using the environments and platforms created by Dominion for this purpose. Never remove information from these environments or platforms without the approval of the head of department, area or division.
- Never use confidential information for their own benefit or for the benefit of another person or organisation.
- Personal passwords shall never be shared or disclosed to anyone other than the authorised user.
- Regularly renew passwords in order to protect them being known to unauthorised users.
- Return access permissions as soon as such access requirements are no longer required, when responsibilities are changed on when employment at Dominion is terminated.

Use of hardware

All computer and communication equipment, whether these be servers, desktop or laptop computers, mobile telephones, data storage units, video conferencing systems, printers, projectors or other communication, IT or audiovisual equipment, whether owned or leased by Dominion, can only be used to carry out the duties and tasks of the corresponding job position. This equipment will be used as a work tool to allow for better and more efficient execution of the work assigned and therefore they cannot be used for any purposes other than these, regardless of whether they are specific or unrelated to the main purpose of Dominion's activities.

Obligated Parties must not save personal data or files on the corporate computer.

Use of Software

Only software and computer applications that have been purchased and provided by Dominion and appropriately licensed by Dominion can be used on the computers that Dominion makes available to the Obligated Parties. Software can only be installed by personnel specifically designated by, or authorised by, the relevant IT department. Installing, saving and using any third-party software not provided by Dominion on these computers is strictly forbidden.
Whenever a Obligated Party considers that, in order to carry out its functions, an application or computer programme is required that has not been installed on their computer, they may request this from the person in charge of their department, area or division, stating the reasons for such a request.

E-mail

E-mail must only be used for business purposes in relation to Dominion's activity and to fulfil the responsibilities entrusted to the Obligated Subject.
E-mail addresses allocated to Obligated Parties is not considered their property but rather Dominion's, even when it contains the name and surname of the person in question.

Internet

Dominion provides internet services to Obligated Parties primarily as a as an IT resource to perform Dominion business activities and to carry out their professional duties as efficiently as possible.
Access can be restricted to only those websites deemed necessary to carry out their work, and any unwanted websites and address filtering software can be installed.

Other resources

The use of other resources, such as landline and mobile telephones, photocopiers and other types of electronic equipment is also restricted to business use and must comply with any regulations set out by Dominion.

Monitoring and Control

When using its organisational and managerial powers, as well as its power of disposal with regards work resources, Dominion may perform internal audits to check that Obligated Parties make proper use of the company's IT resources, hardware and software, particularly e-mail and internet.
To this regard, measures can be taken at any time to control and prevent - pursuant to current legislation in each country - the improper Internet and e-mail usage, such as regular checks of e-mails sent and received by the Obligated Party, the installation of software to take regular screenshots of the Obligated Party's computer screen, computer alerts and activity logs relating to Internet browsing or sending e-mails, and other measures.

Reporting Wrongdoings

All Obligated Parties and third parties have a Whistleblowing channel to report any conduct that may involve any wrongdoing or any illegal actions or any actions that go against the Code of Conduct or Policy. For further details regarding the Whistleblowing Channel, consult the Code of Conduct.

Document sheet

Document table:

Document Type	Corporate Policy
Document code	PC-04-5.2-09-202111
Date of the document	November 2021

Prepared by:

Name or role	Remarks	Date
Risk & Compliance Department		November 2021

REVISED BY:

Name or role	Remarks / Approved by	Date
Audit and Compliance Committee		

Table of Editions:

Edition	Date	Description