DOM SI S13

Protocol for employees regarding the use of corporate information

Date: 06.06.2023

Process: Support

Instruction: Corporate information management

Code: DOM SI S13

Revision: v07

Document sheet

DOCUMENT TABLE:

Document Type	Protocol
Date of the document	22/06/2022
Last revision	06/06/2023

REVISION	DATE	PREPARED	REVISED	APROVED	OBSERVATIONS SUMMARY OF CHANGES
00	27.03.2023	Iván Cartaya	Estanis Elorrieta	Yago Barandiaran	Initial edition
01	06.06.2023	Rubén Ledo	Estanis Elorrieta	Yago Barandiaran	Review details

Contents

1. OBJECT AND PURPOSE

The purpose of this protocol is to establish the company's general policy with regard to the security of corporate information and to identify best information management practices in accordance with the body of regulations represented by the regulations in force in the different places in which Dominion is operating and, specifically, by European General Data Protection Regulation 679/2016 (hereinafter GDPR). This is for the purpose of making company employees and directors aware of their obligations and rights with regard to corporate and personal information management.

DOMINION is committed to promoting respect for the processing of the personal data of its employees and directors, as well as that of the users of its services and to ensuring security in the safeguarding of this data. For this reason, all those working for the organisation, or directing or representing it, take on the commitment to comply with the applicable regulations in force.

The practices detailed below are directed at achieving the said purposes and must be applied to the processing of information in general and to personal data in particular, in compliance with the body of information indicated above.

For any doubts regarding the use or transfer of information, the Data Protection Officer can be contacted through the following channel: dpo.corporate@dominion-global.com.

2. CONFIDENTIALITY OF THE INFORMATION.

The information accessed by DOMINION's personnel, whether pertaining to DOMINION, or to customers, suppliers, business partners or partners of any other type, that is related to their day-to-day activity, comprises corporate information and must be accessed solely for the purpose of performing the professional tasks assigned. To this effect, the following mandatory guidelines must be observed.

Conduct Guidelines for personnel

- Keep secret and confidential all the information managed in the organisation. This obligation means that personnel must not disclose, transmit, comment on or express their opinion through any physical, verbal or telematic media, information relating to customers, processes, tools, proposals, business or organisational strategies and any other information that personnel may have access to as a result of their job, and unless authorised to do so. Personnel shall continue to be bound by this obligation to professional secrecy after the termination of their employment relationship, insofar as it constitutes their "know-how" or own knowledge.

- Any documentation, applications, procedures or body of knowledge that may be prepared, executed or put into practice at DOMINION is a corporate asset that is the property of the organisation.

- The systems and applications to be used in the corporate computing devices provided by DOMINION are those determined by the latter. Personnel undertake to comply with the internal rules relating to their use while performing their tasks and in conditions of security, confidentiality and privacy of information.

- It is not permitted to make copies, transmissions, communications transfers or assignments of personal data or corporate information, except for the performance of the duties assigned.

- It is not permitted to modify the settings of the applications or the operating system, neither is it permitted to delete, destroy, damage or alter the content of DOMINION's databases. This modification could lead to the infection of equipment and, therefore, the loss of information. Should an employee require a specific setting or software in order to perform their work, then an official request must be made to the organisation for evaluation and, in such a case, this is made by the IT service.

- Only the service or designated person from the organisation may make communications to publications, the media or social networks, in accordance with the Social Network Policy approved by DOMINION. This also applies to declarations made to public bodies and supervisory authorities, which can only be made by persons authorised to do so or by the company management.

- The company's IT systems and repositories, as well as the tools made available to personnel, shall solely be used for work-related purposes. DOMINION has the right to monitor and, where appropriate, restrict the use of the said devices. If, exceptionally, a member of staff is obliged to store personal information on the said system, then this must be done in a folder that is differentiated from the corporate information and with the title "personal folder + name and surname". In any case, personnel shall manage their folder under the same security rules as those applicable to the management of corporate information, avoiding including in the said folder content that could affect the security of the system.

- Personnel related to DOMINION must comply with the data protection rules and actively contribute to compliance with the same.

3. INFORMATION SECURITY AND THE PROPER USE OF COMPUTING RESOURCES

3.1. Password management

- The daily processing of information in the course of work requires access to different services, devices and applications for which the following pair of credentials is used: access and password. For the security of the services and systems in which there are user accounts, there is a need to guarantee that the authentication credentials generated are updated and revoked optimally and securely.

- Passwords are vital in order to ensure that the entire security system is not compromised. This means that passwords that are either weak or poorly safeguarded can favour unauthorised access and use of an organisation's data and services. Therefore, diligent password management is a legal obligation, the breach of which can lead to severe sanctions, and it is critical for the security of the entire system whenever other more advanced identification and authentication systems are not in place.

Guidelines for password creation and resetting

- A user requiring access to the computerized information systems in order to perform their tasks and responsibilities, shall have an identifier system to access the necessary applications and a password to authenticate the user as having authorised access to the organisation's information systems. The said password shall be provided by the organisation although it may be changed by the user. Dominion personnel may eventually have various independent access systems, managed with various logins if necessary.

- User logins and passwords are personal and non-transferable and their disclosure to third parties is prohibited, unless expressly authorised to do so by DOMINION. In the event of temporary leave, requiring other employees to perform the work, temporary access should be given.

Therefore, with regard to passwords, the following should be taken into account:

- Passwords must not be shared with anyone, and the save password option must not be used.

- Passwords must not be written down on slips of paper or post-its.

- Passwords must not be written in emails or on website forms from an untrusted source.

  Each user shall be responsible for the confidentiality of their password and, should this accidently or fraudulently become known to unauthorised persons, then this must be reported as an incident helpdesk.it@global-dominion.com and changed immediately.

- If the password account holder is absent from work, then temporary access should be granted to the replacement employee.

- Passwords must be robust and, therefore, difficult to guess or calculate. For this reason, they must not contain simple words (names or places), they must have at least 8 characters (lowercase, uppercase, numbers and symbols), they must not be logical chains of characters that can be guessed (dates of birth or similar). It is also advisable to minimise the use of dictionary words given that there are programmes that can crack the password based on documents of this type.

- The passwords of computers connected to the corporate domain shall have a validity of forty-five days (45) and must be changed at the end of this period. An alert notice will be displayed (15) days before expiry.

3.2. Actions at the workstation.

- There is a need to guarantee the security of all the information and resources managed at the workstation, in view of the fact that the management of the information of an organisation is made on many occasions from this point, both from technological devices and also in a more traditional way (paper or phone). This is why it is important to require compliance with certain rules for workstation security.

Access and management of information

- DOMINION personnel must respect the organisation of the information and their access rights to the same, based on their task profiles and without prejudice to contents that are held for specific reasons. In this way, personnel may only access the information systems when so required for the performance of their duties. It is prohibited to share the disks and folders of the user equipment at Dominion, unless there is a justified requirement to do so, given that this practice could lead to the propagation of virus in the network.

- Each employee shall be responsible for their workstation, ensuring that the personal information or corporate information is not transmitted to unauthorised persons, regardless of whether they are employees or unrelated to the organisation.

- It is prohibited to install P2P programmes, used to download music, films and other programmes, in Dominion's equipment.

- Access to and management of processes shall be made in the corporate network storage system (shared disks and Sharepoint sites). Employees must not work with corporate information in local work mode.

- The use of removable devices is not permitted, unless authorised to do so by the head of the DOMINION Business Unit, resulting from service needs and subject to content encryption.

- In order to prevent operating system vulnerabilities, users must apply the updates and security patches released by the manufacturer or, where appropriate, reboot equipment in order to install the updates.

- Likewise, users must ensure that their equipment has a corporate antivirus that has been correctly installed, activated and updated.

- The use of instant messaging systems shall be limited to unimportant matters, such as reminders or alerts or similar. In any case, they must never be used to send corporate information or personal data, unless DOMINION authorises their use to transmit more important information.

- Company information must only be sent using the corporate tools (email, Onedrive, Sharepoint) or any other medium provided by DOMINION or its customers for such purpose.

- In case of using DOMINION's Office 365 data sharing services with third parties, acceptance of the "DOMINION's Office 365 Data Sharing Services Access and Use Policies" must be obtained.

Tidy desk policy

- Avoid storing documents on desks, either tidy them away or dispose of them after use, storing them in suitable material and spaces (classifiers and furniture).

- Limit the printing of documents to those documents that are absolutely necessary.

- Keep any item that could give access to the documents (such as keys or passwords) in the utmost safety and security.

Destruction of sensitive documentation using secure mechanisms

- This shall be performed with paper shredders for the use of employees, given that there are risks associated with the use of waste paper bins for sensitive documents (personal data, financial information, etc.).

- In the case of the mass destruction of documents, the organisation shall make specific services available in order to ensure secure destruction.

Use of printers, scanners, photocopiers and similar items

- Personnel using these items must ensure that no printed documents are left in the output tray or send folder.

- If the printers or scanners are shared by a number of users, then the documents must be removed as soon as possible or deleted from the feeder tray or saved to prevent unauthorised access by others.

Computers security, screen locking and logging-off

- When a person leaves their workstation unattended, either temporarily or at the end of their work shift, then it must be left in a condition that prevents the information on computer-based storage from being viewed by locking the screen or logging-off or ensuring that no documents or other media containing personal information or confidential corporate information are left at the workstation and which could be seen by unauthorised persons. All laptop and desktop computers that are connected to the domain must be automatically locked after ten (10) minutes of inactivity.

- Whenever the computer is at your workstation, it must be protected with the use of a security cable.

- The computer must be switched off at the end of the working day.

Correct use of the internet

Personnel must make diligent use of the Internet, basing its use as a work tool for the performance of their tasks and responsibilities and will follow basic security recommendations such as:

- Check that the (URL) destination addresses are secure and that the address to be used is correct.

- When the connections are to secure environments (web mail, extranet, etc.) or when transactions are made with critical information, check the validity of the certificate and compliance with protocols (https://).

Protection against malware

- It is prohibited to use programmes containing malware on Dominion's network or servers such as (Virus, Worms, Trojans, etc.).

- Although security tools do exist, employees must be careful when opening emails with attached files coming from unknown senders, as these emails could contain virus, trojan programmes or links to steal information or access credentials. If a suspicious file is received, then the IT department should be contacted at the following address: helpdesk.it@dominion-global.com , to analyze the file.

- All information coming from external sources such as pen drives, external disks, Internet or email, must be checked with the antivirus system before use.

Pay attention to the requirements imposed by intellectual property rights

- The resources available on the Internet are subject to the limitations imposed by their authors or proprietors, as indicated in their content. It is therefore necessary to consult the terms and conditions and respect the intellectual property rights.

- DOMINION is committed to respecting the intellectual property rights of computing programmes and applications. For this reason, the use of applications that have not been authorised by the organisation is not permitted, and this software must be correctly licensed.

3.3. Use of email

- The corporate email does not belong to the private sphere of the worker, but rather it is the property of the company, which provides it to the employee for the purpose of carrying out their work activities, thus the company has the right and ability to access its content if necessary. It is important to note that this practice would only be carried out with the aim of protecting the interests of the company and ensuring a suitable and productive work environment. Therefore, it is recommended that employees are aware that their electronic communications at work are not private and that they ensure not to send private information through this medium.

- Email is an essential communication tool for the operation of an organisation and it is necessary to define its correct and secure use. There is a need to raise the awareness of users and to ensure that diligent use is made of emails in the interest of avoiding the risks resulting from the use of the corporate email, such as an unintentional error or an external attack through spam and phishing mails, which try to steal credentials through the use of social engineering techniques that allow the sender to impersonate a specific entity or person in order to achieve their own ends.

Guidelines for the correct use of email

- Identify fraudulent and suspect emails.

- Do not use the corporate email for personal purposes.

- Use a secure password and two-factor authentication for email access.

- Identify the sender before opening the email received; if you think that the identity is suspicious, then contact the sender by another means in order to confirm it. If the email is from outside the organisation, then you should act with greater diligence, previously confirming the address with the sender. "Social engineering" techniques are being used to trick people by sending an email in which the scammer pretends to be another person , institution or company, and uses arguments such as the urgency to perform a transaction, for example. It is particularly important to watch out for the possibility of being faced with this technique and to detect it in time, by not opening attachments and not clicking on suggestions for links, neither should you fill in attached forms or applications without first verifying their source. Enter the URL manually instead of using the links provided in the suspicious messages.

- Analyse the email attachments from unknown senders before opening them. Should you suspect the authenticity of an email or when the message shows changes in design, demands urgent action, invites or requests you to do something unusual or requests access credentials to a website or application (bank account, ERP, etc.) do not open the mail and request instructions from heldesk.it@dominion-global.com

- Inspect the links before opening a message.

- Do not reply to spam. Instead, add it to your spam list and delete it.

- Use the "blind copy" email option to send the same email to multiple recipients so that their email addresses are not shown.

- Do not check the corporate email from public networks.

- Do not re-send corporate mails to personal accounts.

- On termination of the user's employment relationship due to dismissal or resignation, transfer or other causes, the email account shall be locked and an automatic reply mail shall be entered to redirect senders to another corporate address.

3.4. External information management

- External information management through a paper-based or computer-based system is essential in order to maintain the confidentiality and security of the information insofar as the information is taken out of the organisation's facilities for the management of the service.

Guidelines for external information management

- It is permitted to take corporate information out of DOMINION's facilities either on a paper-based medium or computer-based medium for service requirements, as far as is permitted by the organisation.

- During the transfer of documents, there is a need to minimise the risks resulting from the loss, theft or accidental or intentional manipulation. To do so, there is a need to adopt measures directed at preventing access to or the manipulation of the information being transferred. A mechanism that adds protection and, in order to be opened, requires a key or knowing a combination, for example.

- The documentation must be at all times controlled, under the supervision of the person making the transfer, and guarded in order to prevent loss or unauthorised access.

- With regard to computer-based media, the information contained shall be encrypted whenever possible, or else there shall be access passwords that guarantee that the said information cannot be accessed or manipulated during transport or to protect against access in the event that the device is lost.

3.5. Remote Access to Corporate information

- It is essential to guarantee the security of corporate information and communications when access to the information is from devices located outside the physical facilities of DOMINION, through the use of external non-corporate networks.

- Access to DOMINION's information from outside the workplace (travel, meetings, telework, etc.) means that, on occasions, it will not be possible to use the 4G/5G networks or connections, requiring connections to be made through domestic or public networks (hotels, cafeterias, airports, etc.) which may not be secure and, in any case, do not have the security offered by the corporate systems.

- Remote access to the corporate services (network servers) shall be made through a corporate computer and through the establishment of a VPN network set up by the organisation.

- Access to information stored in the company's Sharepoint sites must be made by authentication with the email credentials, duly protected with the used of two-factor authentication.

- If mobile devices are used to work outside DOMINION, then these must be corporate and the necessary security measures must be taken in order to guarantee the security of the same.

3.6. Management of security incidents

The user is responsible for notifying the IT department helpdesk.it@dominion-global.com of any security incident, fault that is affecting or could affect data security, understood to be any event that may occur occasionally and that could involve a loss of data confidentiality, integrity or availability, virus infection or the receiving of emails from unknown senders that could contain malware, content for scams or the theft of access credentials from Dominion's resources or systems. The body responsible for internal compliance shall decide whether it is necessary to notify the supervisory authority and the person(s) affected.

The IT area shall provide an incident register to record any incident that could represent a threat to the information and take corrective measures.

In the event of an incident, DOMINION shall follow a specific process governing security breaches or incidents and shall prepare the corresponding reports in the interest of evaluating the incident.

In order to determine exactly what is to be understood by incident, the most common incidents are mentioned below, by way of example yet without being an exhaustive list:

- Cyberattacks.
- Access to the information by persons who are not part of the action or, in general, unauthorised personnel.
- Virus/malware alerts generated by the antivirus.
- Suspicious phone calls requesting sensitive information.
- Emails containing virus.
- Loss or theft of documentation or mobile devices and external storage devices.
- Compromised confidentiality of system access password.
- Accidental or intentional deletion of information.
- Accidental or intentional alteration of data or records in the applications.
- Anormal behaviour of the information systems.
- Discovery of information in non-designated locations.

- Evidence or suspicion of physical access of unauthorised personnel to restricted access areas (CPD), offices, warehouses or other facilities) or to computing systems or confidential information by third parties.
- Any suspicious or abnormal activity that you may detect at your workstation.

3.7. Liability

- Given the implications and liabilities with regard to criminal, administrative and/or civil liability of organisations, as well as the administrative and/or civil liabilities that could result from the inadequate management of personal data, the directors and employees undertake to implement this protocol and to take it into consideration as well as any other rules established by the organisation and which are applicable in the personal data protection and corporate information areas.

- The non-compliance or inadequate compliance of personal data processing personnel or the unauthorised access by other personnel, may entail liabilities as legally established by the legislation in force.

4. PRIVACY AND THE USE OF THE PERSONAL DATA OF DOMINION PERSONNEL

- Any employee-related data that may be collected or generated is managed for the development and management of the employment relationship, as well as for compliance with the organisation's legal obligations. The said data shall not be transferred to third parties or organisations, except for compliance with any applicable legal obligations, as well as to Group companies, including in the said transfers those subsidiaries that are outside the European Union, on the grounds of the organisation's legitimate interest. Employee-related data may be transferred to third-party companies, including those located outside the European Union or outside the state in which the subsidiary is located, if this is strictly necessary for compliance with the contracts signed by the Group.

- Specifically, should DOMINION produce audiovisual promotional material on the company's activity, with the participation of some of its employees, in order to capture and disseminate information about the organisation's activity either through its corporate website, publications, newsletters, reports, campaigns, social or professional networks or the media, then the person's consent shall be requested with the exception of the directors and members of the corporate bodies, by reason of their corporate activity as representatives of the organisation. As an exception to this provision, any company activity involving participation in fairs, presentations of the company's services or company activities in which its employees are engaged, then it shall be understood that they have given their consent from the time at which such employees actively take part in the filming or photography. In any case, such participation shall be voluntary and participants shall be informed beforehand of the purpose for which the image is to be used, and of its utilisation. Anyone may request the withdrawal of these images by informing the Corporate Communication Department, by email: corporate.communication@dominion-global.com.

- The employee's personal data shall be held for the duration of the employment relationship. Upon termination thereof, such data shall be blocked, with access restricted to authorised personnel, remaining in this situation until the time-barring periods have elapsed for any actions that may result therefrom and for those established in the applicable tax legislation or any other specific legislation applicable to the activity. Notwithstanding this, the basic data of name and surnames, position and period of employment may be kept for historical purposes.

- The data collected are mandatory and a refusal to provide them could lead to the impossibility to enter into and/or to maintain an employment relationship with DOMINION.

- Data subjects have the right to access their personal data, to request the rectification of incorrect data, to request the erasure of the data when among other reasons, the data are no longer necessary for the purpose for which they were collected, to request the restriction of the processing of their data, in which case the data shall only be held for the exercise or defence of legal claims, as well as to object to the processing of their data, in which case DOMINION shall stop processing the data, except for compelling legitimate grounds, the existence of a legal obligation or the exercise or defence of possible legal claims. The data subject also has the right to withdraw consent if the legal grounds for processing are based on consent.

- Should a data subject consider that their rights have not been observed, then they have the right to submit a complaint to DOMINION through email address: dpo.corporate@dominion-global.com with the reference "request to exercise personal data protection rights", for which purpose a sample request is available on website: www.dominion-global.com

- Personnel are responsible for the lawfulness, truthfulness and accuracy of the personal data provided to the organisation and are obliged to inform of any changes to such data. The said data are mandatory for the establishment and development of the employment relationship.

- In those cases in which the company has made a corporate email available to its personnel, then this shall be considered to be an irrefutable means for DOMINION to send communications.