Cybersecurity Policy

Purpose

The purpose of this document is to define the permitted use of the ICT environment of the Port of Antwerp-Bruges, and to guarantee confidentiality, integrity and availability. In concrete terms, this means that specific obligations are imposed on users, and the procedures to be followed in the event of (alleged) infringements are laid down. The Cybersecurity Policy is a basic document. Where necessary or desirable, specific procedures will impose additional rules. These procedures can always be requested via the internal contact person at the Port of Antwerp-Bruges.

Security classification

This document has a security classification of 'Public', which means that there are no restrictions on distribution.

Version history

No.	Description	Adapter	Date
0.1	First draft version	Yannick Herrebaut	20 years 2023
0.2	Second draft version	Elly Buys, Hanne Pauwels, Shauni Willems	18 April 2023
0.3	Latest draft version	Yannick Herrebaut	14 June 2023
1.0	Final version	Yannick Herrebaut	19 June 2023

Scope

The Cybersecurity Policy applies to the entire ICT environment of the Port of Antwerp-Bruges. This includes all ICT resources (laptops, smartphones, telephones, multifunctionals, ...), ICT infrastructure (servers, storage, network equipment, cloud infrastructure, ...), software (databases, applications, unified communication applications, ...), and all data processed, transmitted or stored in these systems.

The Cybersecurity Policy also applies to the external ICT resources, not owned by the Port of Antwerp-Bruges, which are used in combination with the ICT environment of the Port of Antwerp-Bruges, to the extent permitted (e.g. unmanaged laptop and smartphone, external data carriers, etc.).

User accounts

Access to the ICT environment of the Port of Antwerp-Bruges is granted by individual authentication via a user account, based on a Microsoft Windows username and password, in combination with multi-factor authentication. The password policy of the Port of Antwerp-Bruges has been elaborated in a specific policy, which can always be requested via the internal contact person at the Port of Antwerp-Bruges.

The following rules apply:

- The password must be changed regularly and in any case immediately if requested by an authorized employee (such as after a burglary has been detected or if the password is too weak).
- For all applications, choose a complex password that complies with the password policy of the Port of Antwerp-Bruges.
- If there is only a slight suspicion of abuse of the user account, the password must be changed as soon as possible.
- No one may pass on their password to third parties (e.g. interns, job students, other external parties or internal employees, via e-mail, on unknown websites and locations, etc.) and/or have their user account used by third parties.
- No one may use another person's user account.
- Trying to crack or retrieve passwords of other people is prohibited.
- It is not permitted to store or use passwords in visible form (such as on post-its, in unprotected files, etc.).
- Care must be taken when entering passwords (e.g. not when someone is watching, not when you are connected to a public Wi-Fi network, ...).
- The username and password of the Port of Antwerp-Bruges may only be used for access to the network, systems and applications of the Port of Antwerp-Bruges. The same username and/or password may in no way be used on the Internet or on external ICT resources, other usernames and passwords.
- It is not allowed to enter the username/password of the Port of Antwerp-Bruges on devices that have a public character, such as PCs in the "business corner" of a hotel, demo tablets in a store, ...

Everyone is responsible and liable for everything that happens under his/her user account. If there is a serious suspicion that the user would violate the rules described in this Cybersecurity Policy, the Port of Antwerp-Bruges can completely or partially deny access to the ICT environment of the Port of Antwerp-Bruges.

A user account does not have administrative rights. Installation of software on ICT resources of the Port of Antwerp-Bruges must be requested via the Service Desk of the Port of Antwerp-Bruges. If structural administrator rights are required in the context of the assignment, a separate user account for these specific tasks will be provided by the Service Desk of the Port of Antwerp-Bruges and subject to specific approval by the Cyber Resilience Manager.

On some ICT means, it is also permitted to log in in another way in addition to the password, e.g. via PIN code or biometric authentication (fingerprint, facial recognition, ...). The same rules as for a password apply, except for the length and complexity.

Data & communication

User responsibilities

It is strictly forbidden to send data with unlawful and/or inappropriate content (namely obscene, racist, xenophobic or discriminatory in nature). Spam or suspected malicious messages must be reported to the Port of Antwerp-Bruges by means of the appropriate buttons in Outlook.

The user should exercise caution to ensure that software and data obtained from unknown or unreliable sources, such as an external network, web applications (e.g. Sharepoint, FTP server, ...), external ICT resources (e.g. smartphones, tablets, laptops, ...) or portable media (e.g. USB sticks, memory cards, external hard drives, ...), to the extent permitted, do not contain malware. When a user is confronted with malware, a suspicious document, or a document of unknown origin, work must be stopped immediately and the Servicedesk of the Port of Antwerp-Bruges or the user's internal contact person, whichever is most appropriate at that time, must be contacted.

The mailbox of the Port of Antwerp-Bruges is only for professional use. To conduct personal communication, a separate e-mail address must be used (e.g. Gmail, Outlook.com, ...). The same applies to the registration of personal accounts (e.g. Facebook, Apple, Google, etc.). All data that the user stores under his user account in the ICT environment of the Port of Antwerp-Bruges are considered professional, and can be requested by employees of the Port of Antwerp-Bruges if necessary. Internet access is provided for professional purposes only. The Port of Antwerp-Bruges reserves the right to block certain websites, of whatever nature, if this benefits the protection of its infrastructure and its reputation.

Handling information

All data provided by the Port of Antwerp-Bruges, and all enriched, processed and derived data, are and remain at all times the exclusive property of the Port of Antwerp-Bruges, even if these data, or parts thereof, are enriched, processed or derived by means of the results, which are designed/made available in the context of the Assignment. Unless otherwise specified, these data are confidential information within the meaning of the article "Confidentiality" of these specifications.

Only the Port of Antwerp-Bruges can determine how this data is stored, accessed, copied, edited, distributed and exploited, at its own discretion, both during and after the execution of the assignment.

Hardware

Users who need to be able to access relevant information, mobile and at any time for the execution of their assignment, may be assigned a laptop from the Port of Antwerp-Bruges. This laptop is a work

device, intended to perform purely professional tasks. The device is centrally managed by the Port of Antwerp-Bruges and users do not have administrator rights themselves.

The user has a number of responsibilities in terms of the use of ICT resources:

- Keeping the ICT resources that have been made available in good condition. We apply the general principle of 'good family man' for this;
- Do not leave unattended the ICT resources made available (e.g. in the lobby of a hotel, in a restaurant, in the station, (visible) in the car, ...) and take sufficient security measures to prevent theft or loss as much as possible. In the event of theft or loss, the service desk of the Port of Antwerp-Bruges must be contacted as soon as possible via the ICT Servicedesk or by telephone. In the event of theft, the user must always have a police report drawn up. In the event of loss as well as theft, the Port of Antwerp-Bruges may choose to ask the user or his employer for compensation;
- When leaving an ICT device (e.g. to go to the toilet, get a coffee, go to the printer, ...) this must be locked.
- No software may be installed on the ICT resources made available on the user's own initiative. This also includes extensions and plug-ins for browsers that have not been explicitly approved by the Port of Antwerp-Bruges.

The ICT resources are made available for as long as, in the opinion of the Port of Antwerp-Bruges, their use is professionally required. Is at any time, in the opinion of the Port of Antwerp-Bruges, one or more ICT resources no longer required for a proper implementation of the user's assignment, or if the user is absent (for a long time) (holiday, illness, ...), or if it is established that the user does not or does not correctly use the ICT tool provided, at the first request of the Port of Antwerp-Bruges, the user will return the ICT resource(s) in an orderly state.

In all cases where withdrawal of the ICT asset is justified, the ICT asset with all accessories must be returned in an orderly state. If the ICT asset is not returned, not returned on time and/or not in proper and complete condition, the user is liable for the damage that the Port of Antwerp-Bruges may suffer as a result. The Port of Antwerp-Bruges reserves the right to claim compensation in that case.

In the event of suspicions of intentional, gross damage to the ICT asset, the Port of Antwerp-Bruges may decide to discontinue the cooperation, without prejudice to its right to claim compensation for the damage suffered.

Expressly prohibited

The Cybersecurity Policy of the Port of Antwerp-Bruges explicitly prohibits:

Hardware

- allow the ICT tool provided to be used by a third party, such as family members;
- Use USB sticks, external hard drives and other data carriers in combination with the ICT resources of the Port of Antwerp-Bruges, unless expressly permitted in writing by the Port of Antwerp-Bruges;
- reinstall the laptop yourself. In case of problems with the laptop, the Servicedesk of the Port of Antwerp-Bruges must be contacted.

Data

- store or distribute data that:
  - may damage the image, moral or economic interests of the Port of Antwerp-Bruges.
  - is offensive, defamatory, offensive or discriminatory in nature (e.g. pornography, extreme violence, discriminatory messages, ...)
  - may cause damage to third parties;
  - is in violation of the applicable legislation (e.g. the GDPR, copyright or in the field of electronic communications);
- edit data so that:
  - the image, moral or economic interests of the Port of Antwerp-Bruges are damaged.
  - it becomes offensive, defamatory, offensive or discriminatory in nature (e.g. pornography, extreme violence, discriminatory messages, ...)
  - this may cause damage to third parties;
  - it is in violation of applicable legislation (e.g. GDPR, copyright or in the field of electronic communications);
- pass on company data (e.g. internal documents, unpublished research results, trade secrets, personal data, etc.) to persons who are not entitled to receive, distribute or publish this data;
- to store or transfer company data or personal data unprotected, both electronically and on paper;
- to copy all or part of company data, for purposes other than work-related applications, to personal locations in the ICT environment of the Port of Antwerp-Bruges, to which other employees do not have access;
- to copy company data to personal locations outside the ICT environment of the Port of Antwerp-Bruges;
- strictly pass on personal data to third parties (e.g. passwords, PIN codes, private keys, ...) .

Software

- pass on acquired rights of use and licenses of the Port of Antwerp-Bruges to third parties;
- install or use software for which the Port of Antwerp-Bruges has not granted permission or for which there is no adequate license;
- violate copyright and other intellectual property laws (e.g. by copying software);
- to commercialize internally developed software, which has been developed within the framework of the assignment, or to take actions that enable further use or exploitation, unless expressly agreed otherwise in the specifications and/or an agreement with the Port of Antwerp-Bruges.

Email

- send e-mails in the context of a professional activity that is foreign to the user's relationship with the Port of Antwerp-Bruges;
- send e-mails that contain publicity, separate from the Port of Antwerp-Bruges' own commercial activities;
- send e-mails related to games and betting, narcotics, political views or forms of fraud;
- send e-mails that, outside the cases of normal communication within the Port of Antwerp-Bruges, can be considered unwanted or unsolicited (e.g. advertising, spam, chain letters, etc.)

- knowingly clicking on links in emails or opening attachments, while the sender of the email is unknown, or the content can reasonably be labeled as suspicious, malicious or phishing.

Internet

- consult websites whose content is contrary to the principles of the European Convention on Human Rights (e.g. incitement to terrorism, racism, etc.);
- consult websites with content that is legal, but does not fit within a professional context (e.g. erotic or pornographic content, weapons, gambling, etc.);
- consult websites that contain illegal content (e.g. films, series, games, ...) or content that may cause a security incident.
- consult websites that have nothing to do with the assignment.

Hacking

- assume a false identity in the ICT environment of the Port of Antwerp-Bruges;
- obtain data and passwords from employees and third parties by unauthorized means (e.g. phishing, sniffing, internal hacking, etc.).
- circumvent or disable security measures (e.g. anti-malware, firewall, automatic updates, etc.);
- knowingly design, install and/or encourage other (external) employees to use malicious software (e.g. ransomware, trojans, viruses, cryptominers, etc.) on the ICT environment of the Port of Antwerp-Bruges;
- knowingly force unauthorized access to systems to which one is not entitled;
- facilitate third parties to undertake hacking attempts, including by changing, deleting or passing on system information, system configuration, software or files, if one is not entitled to do so under his assignment;
- knowingly disturb workers or other service providers in the performance of their activities or to make attempts to disrupt the ICT environment of the Port of Antwerp-Bruges (e.g. overloading a network or computer, attempts to cause a system to fail, etc.);
- Link ICT resources that are not owned by the Port of Antwerp-Bruges to the network without prior permission from the Port of Antwerp-Bruges, except in those cases where the ICT infrastructure has been developed to allow this (e.g. public Wi-Fi network);

Exceptions

Any exception to this policy must be requested and explicitly obtained in advance and in writing from the Cyber Resilience Manager of the Port of Antwerp-Bruges. Only the Cyber Resilience Manager can allow exceptions. This is a favour, not a right. The exception can be revoked at any time.

Penalties

In order to avoid, stop and/or limit possible damage of any kind, the Digital & Innovation department of the Port of Antwerp-Bruges has the right to immediately take all necessary technical measures when a breach of the Cybersecurity Policy is detected .

In addition, infringements may give rise to penalties, cumulatively if necessary, in accordance with the provisions contained in the specifications or the general terms and conditions of purchase when requesting a quotation or a purchase order.