Cybersecurity Policy

Doel

Het doel van dit document is om het geoorloofd gebruik van de ICT-omgeving van de Haven van Antwerpen-Brugge te definiëren, en confidentialiteit, integriteit en beschikbaarheid te garanderen. Concreet betekent dit dat specifieke verplichtingen voor gebruikers worden opgelegd, en dat te volgen procedures bij (vermeende) inbreuken worden vastgelegd. Deze Cybersecurity Policy vormt een basisdocument. Waar nodig of wenselijk zullen specifieke procedures bijkomende regels opleggen. Deze procedures zijn steeds opvraagbaar via de interne contactpersoon bij de Haven van Antwerpen-Brugge.

Veiligheidsclassificatie

Dit document heeft een veiligheidsclassificatie “Publiek”, waardoor er geen beperkingen op verspreiding zijn.

Versiegeschiedenis

Nr.	Beschrijving	Bewerker	Datum
0.1	Eerste draft versie	Yannick Herrebaut	20 januari 2023
0.2	Tweede draft versie	Elly Buys, Hanne Pauwels, Shauni Willems	18 april 2023
0.3	Laatste draft versie	Yannick Herrebaut	14 juni 2023
1.0	Finale versie	Yannick Herrebaut	19 juni 2023

Toepassingsgebied

De Cybersecurity Policy is van toepassing op de volledige ICT-omgeving van de Haven van Antwerpen-Brugge. Dit omvat alle ICT-middelen (laptops, smartphones, telefoons, multifunctionals, …), ICT-infrastructuur (servers, storage, netwerkapparatuur, cloudinfrastructuur, …), software (databases, applicaties, unified communication toepassingen, …), en alle gegevens die door die systemen worden verwerkt, verzonden of erin worden opgeslagen.

De Cybersecurity Policy geldt evenzeer voor de externe ICT-middelen, niet-eigendom van de Haven van Antwerpen-Brugge, die men in combinatie met de ICT-omgeving van de Haven van Antwerpen-Brugge gebruikt, in zoverre toegestaan (bv. niet-beheerde laptop en smartphone, externe gegevensdragers, …).

Gebruikersaccounts

Toegang tot de ICT-omgeving van de Haven van Antwerpen-Brugge wordt verleend door individuele authenticatie via een gebruikersaccount, op basis van een Microsoft Windows gebruikersnaam en wachtwoord, in combinatie met multi-factor authenticatie. Het wachtwoordbeleid van de Haven van Antwerpen-Brugge is uitgewerkt in een specifieke policy, steeds opvraagbaar via de interne contactpersoon bij de Haven van Antwerpen-Brugge.

Onderstaande regels zijn van toepassing:

- Het wachtwoord moet regelmatig worden gewijzigd en in elk geval onmiddellijk als dit door een geautoriseerde medewerker wordt gevraagd (zoals bv. na vaststelling van een inbraak of wanneer het wachtwoord te zwak is).
- Kies voor alle toepassingen een complex wachtwoord dat voldoet aan het wachtwoordbeleid van de Haven van Antwerpen-Brugge.
- Wanneer er nog maar een licht vermoeden is van misbruik van de gebruikersaccount, moet het wachtwoord zo snel mogelijk gewijzigd worden.
- Niemand mag zijn wachtwoord aan derden (bijvoorbeeld stagiairs, jobstudenten, andere externen of interne medewerkers, via e-mail, op onbekende websites en locaties, …) doorgeven en/of zijn gebruikersaccount door derden laten gebruiken.
- Niemand mag de gebruikersaccount van een andere persoon gebruiken.
- Wachtwoorden van andere personen proberen te kraken of te achterhalen is verboden.
- Het is niet toegelaten om wachtwoorden in zichtbare (zoals bv. op post-its, in onbeschermde bestanden, …) vorm op te slaan of te gebruiken.
- Er dient omzichtig omgegaan te worden bij het ingeven van wachtwoorden (bv. niet als iemand toekijkt, niet wanneer je verbonden bent met een openbaar wifi-netwerk, …).
- De gebruikersnaam en het wachtwoord van de Haven van Antwerpen-Brugge mogen enkel en alleen aangewend worden voor toegang tot het netwerk, systemen en toepassingen van de Haven van Antwerpen-Brugge. Dezelfde gebruikersnaam en/of wachtwoord mogen geenszins worden gebruikt op het Internet noch op externe -ICT-middelen andere gebruikersnamen en wachtwoorden.
- Het is niet toegelaten om de gebruikersnaam/wachtwoord van de Haven van Antwerpen-Brugge in te geven op apparaten die een publiek karakter hebben, zoals PC's in de "business corner" van een hotel, demo tablets in een winkel, ...

Iedereen is verantwoordelijk en aansprakelijk voor alles wat onder zijn/haar gebruikersaccount gebeurt. Wanneer er een ernstig vermoeden bestaat dat de gebruiker de regels beschreven in deze

Cybersecurity Policy zou schenden, kan de Haven van Antwerpen-Brugge de toegangen tot de ICT-omgeving van de Haven van Antwerpen-Brugge volledig of gedeeltelijk ontzeggen.

Een gebruikersaccount heeft geen beheerdersrechten. Installatie van software op ICT-middelen van de Haven van Antwerpen-Brugge dient aangevraagd te worden via de Servicedesk van de Haven van Antwerpen-Brugge. Indien er in het kader van de opdracht structurele beheerdersrechten zouden nodig zijn, zal er door de Servicedesk van de Haven van Antwerpen-Brugge en mits specifieke goedkeuring van de Cyber Resilience Manager, een aparte gebruikersaccount voor deze specifieke taken worden voorzien.

Op sommige ICT-middelen is het eveneens toegestaan om, naast het wachtwoord, ook op een andere wijze aan te melden, bv. via PIN-code of biometrische authenticatie (vingerafdruk, gezichtsherkenning, …). Dezelfde regels als voor een wachtwoord zijn van toepassing, met uitzondering van de lengte en complexiteit na.

Gegevens & communicatie

Verantwoordelijkheden van de gebruiker

Het is ten strengste verboden gegevens te versturen met een onrechtmatige en/of ongepaste inhoud (namelijk obsceen, racistisch, xenofoob of discriminerend van aard). Spam of vermeende kwaadaardige berichten moeten zonder meer gerapporteerd worden aan de Haven van Antwerpen-Brugge d.m.v. de geschikte knoppen in Outlook.

De gebruiker dient de nodige voorzichtigheid aan de dag te leggen om zich te vergewissen dat software en data verkregen via onbekende of onbetrouwbare bronnen, zoals een extern netwerk, webtoepassingen (bv. Sharepoint, FTP-server, …), externe ICT-middelen (bv. smartphones, tablets, laptops, …) of draagbare media (bv. USB-sticks, geheugenkaarten, externe harde schijven, ...), in zoverre toegestaan, geen malware bevatten. Wanneer een gebruiker geconfronteerd wordt met malware, een verdacht document, of een document van onbekende oorsprong, moet onmiddellijk worden gestopt met werken en moet er contact worden opgenomen met de Servicedesk van de Haven van Antwerpen-Brugge of via de interne contactpersoon van de gebruiker, wat op dat moment het meest aangewezen is.

De mailbox van de Haven van Antwerpen-Brugge dient enkel voor professioneel gebruik. Voor het voeren van persoonlijke communicatie, dient een afzonderlijk e-mail adres gebruikt te worden (bv. Gmail, Outlook.com, …). Idem voor wat betreft de registratie van persoonlijke accounts (bv. Facebook, Apple, Google, …). Alle gegevens die de gebruiker onder zijn gebruikersaccount bewaart in de ICT-omgeving van de Haven van Antwerpen-Brugge worden beschouwd als professioneel, en kunnen door medewerkers van de Haven van Antwerpen-Brugge worden opgevraagd indien nodig. Internettoegang wordt enkel verleend voor professionele doeleinden. De Haven van Antwerpen-Brugge behoudt zich het recht om bepaalde websites, van welke aard dan ook, te blokkeren indien dit de bescherming van haar infrastructuur en haar reputatie ten goede komt.

Omgaan met informatie

Alle data aangebracht door de Haven van Antwerpen-Brugge, en alle verrijkte, bewerkte en afgeleide data, zijn en blijven te allen tijde exclusieve eigendom van de Haven van Antwerpen-Brugge, zelfs al worden deze data, of delen ervan, verrijkt, bewerkt of afgeleid door middel van de resultaten, die worden ontworpen/ ter beschikking gesteld in het kader van de Opdracht.

Deze data, ongeacht of ze (al dan niet) als vertrouwelijk gemarkeerd zijn, betreffen confidentiële informatie, die niet mogen worden gedeeld met derden.

Alleen de Haven van Antwerpen-Brugge kan bepalen hoe deze data worden bewaard, ontsloten, gekopieerd, bewerkt, gedistribueerd, en geëxploiteerd, naar eigen inzicht, zowel tijdens als na de uitvoering van de Opdracht.

Hardware

Gebruikers die voor de uitvoering van hun opdracht mobiel en op elk tijdstip toegang moeten kunnen hebben tot relevante informatie krijgen mogelijks een laptop van de Haven van Antwerpen-Brugge toegewezen. Deze laptop is een werktoestel, bedoeld om zuiver professionele taken uit te voeren. Het toestel wordt centraal beheerd door de Haven van Antwerpen-Brugge en gebruikers hebben zelf geen beheerdersrechten.

De gebruiker heeft een aantal verantwoordelijkheden op vlak van het gebruik van ICT-middelen:

- Het in goede toestand bewaren van de ICT-middelen die ter beschikking werden gesteld. We hanteren hiervoor het algemene beginsel van 'goede huisvader';
- Niet onbeheerd achterlaten van de ter beschikking gestelde ICT-middelen (bv. in de lobby van een hotel, in een restaurant, in het station, (zichtbaar) in de wagen, …) en het nemen van voldoende veiligheidsmaatregelen om diefstal of verlies ervan maximaal te verhinderen. Bij diefstal of verlies moet de servicedesk van de Haven van Antwerpen-Brugge zo snel mogelijk gecontacteerd worden via het ICT-loket of telefonisch. Bij diefstal moet de gebruiker steeds een proces-verbaal laten opmaken. Bij zowel verlies als diefstal kan de Haven van Antwerpen-Brugge ervoor opteren om de gebruiker of diens werkgever een schadevergoeding te vragen;
- Bij het achterlaten van een ICT-middel (bv. om naar toilet te gaan, een koffie te halen, naar de printer te gaan, …) dient dit vergrendeld te worden.
- Op eigen initiatief mag geen software worden geïnstalleerd op de ter beschikking gestelde ICT-middelen. Hieronder vallen ook extensies en plug-ins voor browsers die niet expliciet door de Haven van Antwerpen-Brugge zijn goedgekeurd.

De ICT-middelen worden ter beschikking gesteld zolang naar het oordeel van de Haven van Antwerpen-Brugge het gebruik hiervan professioneel vereist is. Is op enig moment naar het oordeel van de Haven van Antwerpen-Brugge één of meerdere ICT-middelen niet meer vereist voor een goede invulling van de opdracht van de gebruiker, of als de gebruiker (langdurig) afwezig is (vakantie, ziekte, …), of als wordt vastgesteld dat de gebruiker het aangereikte ICT-middel niet of niet correct blijkt te gebruiken, zal de gebruiker op eerste verzoek van de Haven van Antwerpen-Brugge de (het) ICT- middel(en) in ordentelijke staat terug bezorgen.

In alle gevallen waarin inname van het ICT-middel gerechtvaardigd is, dient het ICT-middel met alle toebehoren in ordentelijke staat geretourneerd te worden. Indien het ICT-middel niet, niet tijdig en/of niet in behoorlijke en volledige staat wordt ingeleverd, is de gebruiker aansprakelijk voor de schade die de Haven van Antwerpen-Brugge hierdoor mocht lijden. De Haven van Antwerpen-Brugge behoudt zich het recht voor om in dat geval een schadevergoeding te vorderen.

Bij vermoedens van opzettelijke, grove beschadiging van de laptop, kan de Haven van Antwerpen-Brugge beslissen om de samenwerking stop te zetten, onverminderd haar recht om een schadevergoeding te vorderen voor de geleden schade.

Uitdrukkelijk verboden

De Cybersecurity Policy van de Haven van Antwerpen-Brugge verbiedt expliciet om:

Hardware

- het ter beschikking gestelde ICT-middel te laten gebruiken door een derde, zoals familieleden;
- USB-sticks, externe harde schijven en andere gegevensdragers te gebruiken in combinatie met de ICT-middelen van de Haven van Antwerpen-Brugge, tenzij uitdrukkelijk en schriftelijk toegestaan door de Haven van Antwerpen-Brugge;
- de laptop zelf opnieuw te installeren. In geval van problemen met de laptop dient de Servicedesk van de Haven van Antwerpen-Brugge gecontacteerd te worden.

Data

- data op te slaan of te verspreiden die:
    - het imago, de morele of economische belangen van de Haven van Antwerpen-Brugge kan schaden.
    - beledigend, lasterlijk, aanstootgevend of discriminerend van aard is (bv. pornografie, extreem geweld, discriminerende boodschappen, …)
    - schade kan toebrengen aan derden;
    - in strijd met de geldende wetgeving (bv. de GDPR, het auteursrecht of in het domein van de elektronische communicatie);
- data te bewerken waardoor:
    - het imago, de morele of economische belangen van de Haven van Antwerpen-Brugge wordt geschaad.
    - deze beledigend, lasterlijk, aanstootgevend of discriminerend van aard wordt (bv. pornografie, extreem geweld, discriminerende boodschappen, …)
    - deze schade kan toebrengen aan derden;
    - deze in strijd is met de geldende wetgeving (bv. de GDPR, het auteursrecht of in het domein van de elektronische communicatie);
- bedrijfsdata (bv. interne documenten, niet gepubliceerde onderzoeksresultaten, bedrijfsgeheimen, persoonsgegevens, …) door te geven aan personen die niet gerechtigd zijn om deze data te ontvangen, te verspreiden of te publiceren;
- om bedrijfsdata of persoonsgegevens onbeschermd te bewaren of door te geven, zowel elektronisch als op papier;
- om bedrijfsdata, voor andere doeleinden dan werk gerelateerde toepassingen, geheel of gedeeltelijk te kopiëren naar persoonlijke locaties in de ICT-omgeving van de Haven van Antwerpen-Brugge, waarop andere medewerkers geen toegang hebben;
- om bedrijfsdata te kopiëren naar persoonlijke locaties buiten de ICT-omgeving van de Haven van Antwerpen-Brugge;
- strikt persoonlijke gegevens door te geven aan derden (bv. wachtwoorden, PIN-codes, private keys, …).

Software

- verkregen gebruiksrechten en licenties van de Haven van Antwerpen-Brugge door te geven aan derden;

- software te installeren of te gebruiken waarvoor de Haven van Antwerpen-Brugge geen toestemming heeft verleend of waarvoor er geen afdoende licentie is;
- de wetgeving over het auteursrecht en andere intellectuele rechten te schenden (bv. door software te kopiëren);
- intern ontwikkelde software, die binnen het kader van de opdracht werd ontwikkeld, te commercialiseren of handelingen te stellen die het verder gebruik of de exploitatie mogelijk maken, tenzij uitdrukkelijk anders overeengekomen in het bestek en/of een overeenkomst met de Haven van Antwerpen-Brugge.

E-mail

- e-mails te verzenden in het kader van een professionele activiteit die vreemd is aan de opdracht van de externe medewerker met de Haven van Antwerpen-Brugge;
- e-mails te verzenden die een publiciteit inhouden, los van de eigen commerciële activiteiten van de Haven van Antwerpen-Brugge;
- e-mails te verzenden die verband houden met spelen en weddenschappen, verdovende middelen, politieke standpunten of vormen van fraude;
- e-mails te verzenden die, buiten de gevallen van de normale communicatie binnen de Haven van Antwerpen-Brugge, als ongewenst of ongevraagd kunnen beschouwd worden (bv. reclame, spam, kettingbrieven, …)
- willens en wetens op links in e-mails te klikken of bijlages te openen, terwijl de afzender van de mail onbekend is, of de inhoud redelijkerwijze als verdacht, kwaadaardig of phishing kan bestempeld worden.

Internet

- websites te consulteren waarvan de inhoud in strijd is met de beginselen uit het Europees verdrag tot bescherming van de rechten van de mens (bv. het aanzetten tot terrorisme, racisme, …);
- websites te consulteren met inhoud die weliswaar legaal is, maar niet past binnen een professionele context (bv. erotische of pornografische inhoud, wapens, gokken, …);
- websites te consulteren die illegale inhoud bevat (bv. films, series, games, …) of inhoud die een veiligheidsincident kan veroorzaken.
- websites te consulteren die niets te maken hebben met de opdracht.

Hacking

- een valse identiteit aan te nemen in de ICT-omgeving van de Haven van Antwerpen-Brugge;
- via ongeoorloofde manieren (bv. phishing, sniffing, interne hacking, …) gegevens en wachtwoorden van medewerkers en derden te verkrijgen.
- beveiligingsmaatregelen (bv. antimalware, firewall, automatische updates, …) te omzeilen of uit te schakelen;
- schadelijke software (bv. ransomware, trojans, virussen, cryptominers, …) op de ICT-omgeving van de Haven van Antwerpen-Brugge te ontwerpen, willens en wetens te installeren en/of andere (externe) medewerkers aan te zetten deze software te gebruiken;
- willens en wetens ongeoorloofde toegang te forceren tot systemen waartoe men niet gerechtigd is;

- derden te faciliteren om pogingen tot hacking te kunnen ondernemen, o.a. door systeeminformatie, systeemconfiguratie, software of bestanden te wijzigen, te verwijderen of door te geven, indien men daarvoor uit hoofde van zijn opdracht niet toe is gerechtigd;
- medewerkers of andere dienstverleners willens en wetens te storen bij het uitoefenen van hun activiteiten of pogingen te ondernemen om de ICT-omgeving van de Haven van Antwerpen-Brugge te verstoren (bv. een netwerk of computer overbelasten, pogingen om een systeem te doen falen, …);
- ICT-middelen die geen eigendom zijn van de Haven van Antwerpen-Brugge te koppelen aan het netwerk zonder voorafgaandelijke toestemming van de Haven van Antwerpen-Brugge, tenzij in die gevallen waar de ICT-infrastructuur is uitgewerkt om dit toe te laten (bv. publiek wifi netwerk);

Uitzonderingen

Elke uitzondering op dit beleid, dient aangevraagd én uitdrukkelijk, voorafgaand en schriftelijk bekomen te worden bij de Cyber Resilience Manager van de Haven van Antwerpen-Brugge. Enkel de Cyber Resilience Manager kan uitzonderingen toestaan. Dit betreft dan een gunst, geen recht. De uitzondering kan op elk moment, worden ingetrokken.

Straffen

Om incidenten te vermijden, te stoppen en/of om mogelijke schade, van welke aard dan ook te voorkomen of beperken, heeft de dienst Digital & Innovation van de Haven van Antwerpen-Brugge het recht om onmiddellijk alle nodige technische maatregelen nemen, wanneer een inbreuk op de Cybersecurity Policy wordt vastgesteld.

Bovendien kunnen inbreuken aanleiding geven tot straffen, desgevallend cumulatief, in overeenstemming met de bepalingen zoals opgenomen in het bestek, resp. de algemene aankoopvoorwaarden bij de aanvraag tot indienen van een offerte of een inkooporder.