ICS VISA MasterCard
INTERNATIONAL CARD SERVICES

Informatie-beveiliging

Gedragsregels en richtlijnen

Voorwoord

Beste collega's,

Informatie en informatiesystemen behoren tot de belangrijkste activa van ICS. Het waarborgen van de geheimhouding, integriteit en beschikbaarheid van informatie en informatiesystemen is van essentieel belang voor onze reputatie als betrouwbare, zakelijke partner en daarmee eveneens voor de voortzetting van de groei en het succes van ICS.

Door gebruikmaking van computers, e-mail en internet worden informatie en informatiesystemen blootgesteld aan bedreigingen, zoals te makkelijke wachtwoorden, social engineering, phishing e-mails en rondslingerende documenten. Als deze bedreigingen niet goed in de hand worden gehouden, kan dit leiden tot incidenten waardoor ICS aanzienlijke financiële- en/of reputatieschade wordt berokkend.

Informatiebeveiliging is een integraal onderdeel van onze bedrijfsvoering. Wij moeten dan ook gezamenlijk de verantwoordelijkheid nemen voor de beveiliging van informatie en informatiesystemen van ICS. Iedereen heeft een rol te vervullen bij het waarborgen van de integriteit en privacy van klantgegevens, het juiste gebruik van gegevens en het voldoen aan alle wet- en regelgeving.

Om te zorgen dat de informatie die ICS in beheer heeft goed beveiligd wordt, heeft ICS gedragsregels geformuleerd die voor iedereen gelden. Het is belangrijk dat je op de hoogte bent van deze gedragsregels die in dit boekje nader zijn toegelicht.

Namens de directie,

Gijs Wildeboer

CEO

10 Gedragsregels Informatiebeveiliging

Alle medewerkers bij ICS (intern of extern) hebben de verantwoordelijkheid om zorgvuldig om te gaan met (klant)data en de ICS informatiesystemen. Dit moet verankerd zijn in de manier waarop wij werken. Om de beveiliging van de informatie en de informatiesystemen van ICS te borgen zijn er tien gedragsregels geformuleerd waaraan iedereen zich moet te houden:

1. Ga veilig om met je user-id en passwords
2. Ga veilig om met Internet
3. Ga veilig om met e-mail
4. Ga zorgvuldig om met bedrijfsvertrouwelijke gegevens
5. Ga zorgvuldig om met Hardware, Software en Bestanden
6. Weet wat je plaatst op social media
7. Zorg voor een Clean Desk
8. Wees verdacht op Social Engineering en Phishing
9. Ga zorgvuldig om met je toegangspas
10. Meld en begeleid bezoekers altijd

We lichten ze op de volgende pagina's een voor een nader toe.

1. Ga veilig om met je user-id en passwords

Voor onze bedrijfsvoering maken wij gebruik van veel verschillende systemen. Als je het voor je functie nodig hebt, krijg je een persoonlijke user-id. Daarmee kun je inloggen op het ICS netwerk en kun je gebruikmaken van onze systemen en (software) programma's. Omdat je persoonlijke toegang hebt, mag je je user-id en password niet met anderen uitwisselen. Dat betekent dat je geen user-id van een collega mag gebruiken, ook niet als je daarvoor van hem of haar toestemming hebt gekregen. Hoe voorkom je dat een collega toch per ongeluk via jouw persoonlijke toegang aan het werk is? Dat voorkom je door het password van jouw user-id geheim te houden en je pc altijd te vergrendelen als je je werkplek verlaat. Vergrendelen gaat via Ctrl+Alt+Delete, Enter of Windows-toets + L. Als je vermoedt dat een collega je password kent, verander dit dan zo snel mogelijk. Uiteindelijk ben je zelfverantwoordelijk voor de handelingen die worden verricht vanuit jouw persoonlijke toegang.

Hoe stel je een sterk wachtwoord op?

Wanneer je een wachtwoord instelt, moet je rekening te houden met een aantal vereisten.

- Het wachtwoord is minimaal 10 tekens lang en bevat de volgende vier componenten: hoofdletter, kleine letter, cijfer en speciaal teken (@$!).
- Het wachtwoord mag in de voorgaande 12 maanden niet gebruikt zijn.
- Een wachtwoord lijkt niet op je gebruikersnaam, echte naam of bedrijfsnaam.
- Het wachtwoord is geen volledig woord

2. Ga veilig om met internet

Om gebruik te maken van internet hebben wij onderstaande richtlijnen opgesteld. Dit om misverstanden te voorkomen. Is toegang tot internet belangrijk voor je functie? Vraag deze toegang dan aan bij de ICT-Helpdesk. Wil je in je pauze iets opzoeken op internet? Gebruik dan de speciale internet-pc's. Als je internet gebruikt, zorg dan dat je zeker weet met wie je communiceert. Het kan gebeuren dat iemand zich voordoet als een bekende, maar dat niet is. Verifieer bij twijfel altijd. Als het nodig is, kunnen wij het gebruik van internet controleren.

Hoe ga je om met internet?
De belangrijkste punten:

- ICS stelt het gebruik van internet alleen beschikbaar voor zakelijk gebruik.
- Je bent zelf verantwoordelijk voor je pc of ander medium waarop je internet gebruikt. Gebruik daarom alleen de internetverbinding van ICS.
- Het gebruik van internet mag niet leiden tot een verandering in de standaardinstellingen van je computer of persoonlijke toegang. Websites waarvan je kunt aannemen dat ze nadelige gevolgen kunnen hebben voor het systeem, mag je daarom niet bezoeken.
- Software mag je niet zelf downloaden van internet. Want dit verhoogt de kans op virussen, kan de werking van de standaard-pc verstoren en/of het netwerk overbelasten. Heb je voor je functie bepaalde software van internet nodig? Vraag je leidinggevende dan hiervoor een verzoek in te dienen bij de Business Support desk.
- Gebruik je gegevens of software van internet? Controleer dan vooraf of hier auteursrechten van anderen op rusten. Is dat het geval? Overleg dan met je leidinggevende wat je kunt doen.
- Je mag geen malware, zoals virussen, 'wormen' of 'trojans', op de netwerken of computers van ICS verspreiden.
- Negeer oproepen vanuit internet om plaatjes, post, kettingbrieven of andere producties op elektronische wijze binnen ICS te verspreiden. Ook als een oproep ongevaarlijk of zelfs sympathiek lijkt.
- Deel geen bedrijfsvertrouwelijke informatie op internet. Ook mag je géén gebruikmaken van niet door ICS goedgekeurde cloud-diensten (Zoals Hotmail, Gmail, Prezi en andere Cloud diensten). Bedrijfsvertrouwelijke informatie mag beslist niet op 'straat' komen te liggen, dit moet dus te allen tijde worden voorkomen.
- Moeten er 'externe' (bijvoorbeeld niet door ICS verstrekte) computers op het interne netwerk aangesloten worden? Gebruik daarvoor dan alleen de 'zwarte kabel'. Het interne netwerk heeft meestal een 'blauwe kabel'.

3. Ga veilig om met e-mail

De beleefdheidsnormen van telefonie en schriftelijke communicatie gelden ook voor het e-mailgebruik. Wij maken daarin een onderscheid tussen zakelijke en privédoeleinden.

Zakelijke doeleinden

- E-mail mag je niet gebruiken voor het uitwisselen van bedrijfsvertrouwelijke informatie, dit kan via de door ICS goedgekeurde middelen (neem contact op met de Business Support Desk als je hier vragen over hebt). Of als deze berichten versleuteld zijn met een versleuteltechniek (encryptie) die door ICS is goedgekeurd. Onder bedrijfsvertrouwelijke informatie bedoelen wij hier: "Alle informatie met betrekking tot klanten, personeel en bedrijfsgegevens waarvan je weet of zou moeten weten dat deze niet ter beschikking van derden mogen komen."
- In bijzondere situaties (zoals bij langdurige ziekte) kan, met toestemming van je leidinggevende, je e-mailpostbus worden geopend. Dit kun je later altijd herkennen aan een gereset password. Je map met kenmerk 'privé' openen wij in deze situaties niet en blijft dus te allen tijde privé. Bovenstaande gebeurt altijd volgens het vier ogen principe, onder supervisie van de Information Security Officer.

Privédoeleinden

- E-mail mag je gebruiken voor privédoeleinden als je je aan het volgende houdt:
- Beperk het aantal privé e-mails zoveel mogelijk.
- Vermeld het kenmerk 'privé' in het onderwerp van je privé e-mail.
- Verspreid geen bedrijfsvertrouwelijke informatie via privé e-mail.
- Onderteken een privé e-mail als privépersoon. Verstuur deze dus zonder de standaard ICS ondertekening en alleen met je eigen naam.

Bovenstaande criteria worden automatisch gecontroleerd . Alleen als je privé e-mail voldoet aan deze voorwaarden wordt deze verzonden door ICS. Privé e-mail die niet aan deze voorwaarden voldoen, wordt

niet verzonden. Ander e-mailverkeer zien wij als zakelijke mail en wordt automatisch gemonitord op ongepastheden (in woordgebruik en bloot percentages bij foto's/filmpjes). Dit geldt ook voor alle inkomende e-mailberichten. Bevat een e-mail ongepastheden? Dan geeft het systeem automatisch een signaal af en doen we verder inhoudelijk onderzoek.

4. Ga zorgvuldig om met bedrijfsvertrouwelijke gegevens

Elke afdeling binnen ICS heeft te maken met klantgegevens. Wij gaan ervan uit dat iedereen daar op een integere manier mee omgaat. Hieronder vind je een aantal handvatten voor het omgaan met Card-nummers.

- Je mag geen Card-nummers doorgeven (via e-mail, telefoon, et cetera), verspreiden en/of opslaan. Dit mag alleen als je het nodig hebt voor je werk. Plaats geen klant- of Card-gegevens of privé-informatie op H:\HOME\Copy.
- Verstrek geen Card-nummers aan 'derden', deze krijgen geen beschikking over de Card-nummers, vervaldata en Card Verification waarden.
- Card-houdergegevens die je verstuurt naar externe (reclame)bureaus voor ICS mailings, mogen geen Card-nummers bevatten.
- Zorg ervoor dat er geen volledige Card-nummers staan op onderstaande uitingen:
    - Servicebrieven: alleen de laatste 4 posities van het Card-nummer.
    - Rekeningoverzichten: alleen de laatste 4 posities van het Card-nummer.
    - E-mails naar klanten: alleen de laatste 4 posities van het Card-nummer.
    - PIN Mailers: alleen de laatste 6 posities van het Card-nummer.

Om de privacy van al onze klanten te beschermen mag je geen klantgegevens gebruiken voor privédoeleinden, ook niet van je eigen account.

- Je mag apparatuur, systemen en data alleen gebruiken als je daartoe bevoegd bent en het bij je functie hoort.
- Je mag geen actie uitvoeren op je eigen card(s) of die op die van je partner, familieleden, vrienden en kennissen
- Het niet toegestaan enig gegeven te raadplegen (inzien) zonder rechtmatige grondslag uit je werkzaamheden. Het raadplegen van je eigen gegevens valt hier ook onder.
- Door de afdeling Investigations kunnen controles hierop worden ingericht

5. Ga zorgvuldig om met Hardware, Software en Bestanden

Het spreekt voor zich dat je zorgvuldig omgaat met bedrijfseigendommen. Je mag deze alleen voor bedrijfsdoeleinden gebruiken. Omdat niet iedereen hetzelfde verstaat onder deze begrippen, lichten wij ze kort toe:

- **Hardware:** de computersystemen van ICS. Zoals telecommunicatieapparatuur, pc's, printers en terminals.
- **Software**: de programma's voor de hardware (zoals tekstverwerkers, spreadsheets en adviesprogramma's) waarvan ICS eigenaar is en/of er een gebruiksrecht op heeft.
- **Bestanden:** al onze gegevensverzamelingen die vastgelegd zijn op gegevensdragers die kunnen worden gelezen en waarvan ICS eigenaar is en/of er een gebruiksrecht op heeft.

Voor het gebruik van hard- en/of software en bestanden geldt:

- Het geheel of gedeeltelijk kopiëren van systemen en (software) programma's of gegevensverzamelingen mag alleen als je daartoe bevoegd bent en dit bij je functie hoort. Licentiecontracten verbieden nagenoeg altijd het kopiëren van software en bestanden die in gebruik worden gegeven. Uitzonderingen voor specifieke doeleinden worden altijd uitdrukkelijk genoemd.
- Maak alleen gebruik van apparatuur en programmatuur die de afdeling ICT Supply ter beschikking stelt. Installatie en/of gebruikmaken van apparatuur en programmatuur mag alleen als je daartoe bevoegd bent.

- Stel geen apparatuur, programmatuur en gegevensverzamelingen ter beschikking aan anderen. Dit mag alleen als het management of de directie je hiervoor schriftelijke toestemming heeft gegeven.
- Haal je software of gegevens in je computersysteem (dus ook een laptop) binnen met een cd-rom, USB of online (bijvoorbeeld via internet of e-mail)? In dat geval ben je zelf verantwoordelijk voor de gevolgen. Controleer met virusscanprogramma's die door ICS zijn goedgekeurd dat de binnengehaalde software en gegevens vrij zijn van ongewenste programmatuur (zoals malware of virussen).
- Gebruik hardware, software en bestanden altijd zorgvuldig. Maak je er buiten het gebouw van ICS gebruik van? Dan ben je verplicht zodanige maatregelen te treffen, dat de kans op misbruik of diefstal zo klein mogelijk is. Eventueel misbruik of diefstal moet je direct aan het management of aan je leidinggevende doorgeven.
- Laat ingeschakelde hardware niet zonder toezicht achter. Dit mag wel als deze beveiligd is met een screensaver met password.
- Vermoed of merk je dat er virussen op je pc zitten? Geef dit dan onmiddellijk door aan je leidinggevende en de Business Support desk en houd je hierna strikt aan het beleid voor de afhandeling van computervirussen. Als je een laptop gebruikt, controleer dan geregeld met door ICS goedgekeurde virusscanprogramma's of er virussen aanwezig zijn.
- Sluit alléén met uitdrukkelijke toestemming van ICT Supply externe apparaten, zoals Smartphones, tablets, USB-sticks, -disks of mp3-spelers (dit is geen complete lijst!), aan op een computer.
- Het is niet toegestaan om niet door ICS goedgekeurde cloud-diensten te gebruiken met als doel om gegevens op te slaan of over te hevelen. Denk hierbij o.a. aan Dropbox, GoogleDrive, iCloud, SkyDrive.

6. Weet wat je plaatst op social media

Bij ICS zijn we trots op wat we doen en wie we zijn en dat mag uitgedragen worden. Als je actief bent op social media dan kan het zijn dat je niet alleen privé, maar ook als werknemer van ICS aangesproken wordt. Houd je daarom wel aan onze richtlijnen voor het gebruik van social media op persoonlijke titel. Zo kunnen we voorkomen dat wij en/of onze Card-houders schade ondervinden. Hieronder geven we richtlijnen hoe je in deze en andere gevallen het beste kunt handelen om te voorkomen dat ICS en/of onze Card-houders schade ondervinden.

- Besef dat je ICS vertegenwoordigt. Denk goed na over wat je plaatst, juist ook als het niets met ICS te maken heeft. Zorg dat uitingen niet schadelijk zijn voor onszelf en/of onze Card-houders en leveranciers. Sta erbij stil dat je online gedrag praktisch onuitwisbaar is.
- Wees integer, vermeld bijvoorbeeld op LinkedIn geen mooiere functie dan die je in werkelijkheid uitoefent.
- Geef geen bedrijfsvertrouwelijke informatie over jezelf, ICS of cardhouders prijs.
- Houd rekening met auteursrechten.
- Meld contacten die je niet vertrouwt bij Investigations. Bijvoorbeeld als je sterk het gevoel hebt dat iemand zich voordoet als een ander of verkeerde intenties heeft.

De volledige richtlijnen voor social media vind je op intranet.

7. Zorg voor een Clean Desk

Door strenge wet- en regelgeving moeten wij als financiële dienstverlener zorgvuldig, betrouwbaar en integer met bedrijfsvertrouwelijke informatie omgaan. Vandaar dat wij minimale eisen hebben gesteld aan een opgeruimde werkplek. Dit wordt ook wel de 'Clean Desk Policy' genoemd. Wat houdt dit in?

- Laat aan het einde van de werkdag je werkplek leeg achter.
- Berg al je (persoonlijke) spullen en (bedrijfsvertrouwelijke)informatie op in afgesloten ladeblokken of kasten op de afdeling (houd hierbij

Zorg ervoor dat bedrijfsvertrouwelijke informatie niet zomaar gelezen, gekopieerd of meegenomen kan worden. We gaan bij ICS als volgt om met bedrijfsvertrouwelijke informatie:

- Gooi papier dat je verder niet meer nodig hebt niet in de prullenbak maar in de daarvoor bestemde papiercontainers.
- Houd rekening met wat je aan de muur hangt (bijv. op een plannings- of Kanban bord), denk hierbij aan bedrijfsvertrouwelijke informatie.
- Heb je gewerkt met documenten met geheime of bedrijfsvertrouwelijke informatie (bijvoorbeeld klantgegevens)? Vernietig deze dan, zodat de informatie niet te herleiden is. Gebruik daarvoor een papierversnipperaar of gooi de documenten in de papiercontainer. De containers staan op iedere afdeling (meestal naast de kopieermachines). De papierversnipperaar vind je op de afdeling Facility Services.
- Wil je iets printen? Gebruik dan je persoonlijke code, zodat documenten niet door het pand gaan zwerven. Log na het printen altijd weer uit.

Als iedereen zich hieraan houdt, voorkomen we dat 'derden' en onbevoegden inzicht krijgen in bedrijfsvertrouwelijke informatie.

8.Wees verdacht op Social Engineering en Phishing

In toenemende mate proberen criminelen onder valse voorwendselen bedrijfsvertrouwelijke gegevens te bemachtigen om daarmee schadelijke acties uit te voeren. Dit wordt social engineering genoemd. Social engineering richt zich op de zwakste schakel van de beveiliging: de mens. Een social engineering aanval kan op diverse manieren plaatsvinden zoals via e-mail, social media, telefonisch of een persoonlijke benadering. Je wordt bijvoorbeeld gemaild of gebeld door iemand die zich voordoet als een collega of andere vertrouwde persoon die met een 'goede reden' om je wachtwoord of om andere bedrijfsvertrouwelijke informatie vraagt. Wees hierop verdacht: geef nooit je user-id en password en verstrek ook nooit bedrijfsvertrouwelijke informatie aan iemand buiten ICS of iemand wiens identiteit niet kan worden gecontroleerd. Zet ook geen gegevens op internet die criminelen kunnen misbruiken. Bijvoorbeeld het vertellen dat je op een bepaalde afdeling werkt kan criminelen al op het idee brengen om een social engineering aanval op jou te richten.

Phishing is een vorm van social engineering. Bij phishing doet iemand zich voor als een betrouwbare partij om je gegevens te ontfutselen. Dit gebeurt veelal via de e-mail maar kan ook per sms of telefonisch plaatsvinden. Hieronder vind je een aantal tips met betrekking tot phishing:

- Controleer altijd de afkomst van een e-mail die je ontvangt.
- Ken je de persoon of bedrijf die de e-mail zendt?
- Hoort het onderwerp in de e-mail bij je werkzaamheden?
- Verwacht je een e-mail over dit onderwerp?
- Bij een phishing e-mail is de aanhef meestal geachte heer/mevrouw. Maar in het geval van social engineering kan het zo zijn dat je naam al bekend is, waardoor je wel persoonlijk wordt aangesproken.
- Wees voorzichtig met het openen van bijlagen en links in mails die je niet direct vertrouwd.
- Check voor het openen van een link de domeinnaam (waar gaat hij heen?).

- Herken een phishing mail aan het feit dat er vaak wordt gevraagd om iets snel te doen, bijvoorbeeld hulp verstrekken of er wordt gedreigd dat je geen toegang meer hebt als je niet snel een bepaalde actie uitvoert.
- Geef je niet op voor mailinglists en stuur geen kettingbrieven door. Social engineers kunnen op zoek zijn naar e-mailadressen om je vervolgens persoonlijk te benaderen. Laat geen e-mailadressen op internet achter, bijvoorbeeld op fora. Wees ook voorzichtig met het opgeven voor nieuwsbrieven. Hetzelfde geldt voor andere informatie zoals telefoonnummers. Social engineers zijn namelijk zeer behendig in het (automatisch) vinden van deze gegevens.
- Geef nooit persoonlijke informatie in reactie op een e-mail waarin wordt gezegd dat je iets hebt gewonnen.
- Gebruik je gezonde verstand. Vertrouw je iets niet? Neem contact op met de Business Support desk (11510).

9. Ga zorgvuldig om met je toegangspas

Werk je in het ICS gebouw dan krijg je, na positieve screening, van ons een toegangspas. Je hebt daarmee toegang tot de panden en - als je bij ons in vaste dienst bent - ons parkeerterrein. De toegangspassen zijn persoonlijk. Je mag ze niet uitlenen aan collega's of externe partijen. Bij aankomst en vertrek uit pand I of III moet je de toegangspas altijd tegen de pas lezer bij de deur houden.

Meld het verlies van je toegangspas altijd direct bij de receptie, die blokkeren dan je pas en zorgen ervoor dat je een nieuwe krijgt. Als je je toegangspas bent vergeten, krijg je bij de receptie een tijdelijke vervangende pas. Aan het eind van je werkdag lever je deze weer in. Houd er rekening mee dat je je moet kunnen identificeren alvorens de receptie je een tijdelijke pas geeft. Indien de medewerker zich niet kan identificeren bestaat de mogelijkheid dat de receptie een medewerker voorziet van een bezoekerspas, en geen toegangspas uitgeeft. Dit is om te voorkomen dat toegangsrechten aan de verkeerde persoon worden toegewezen. Een toegangspas van ICS kan voor onbevoegden zeer interessant zijn. Zet daarom op je pas geen informatie waaruit blijkt dat het om een toegangspas voor het pand van ICS gaat. Het antwoordnummer achter op de pas verwijst daarom ook niet naar ons bezoekadres.

10. Meld en begeleid bezoekers altijd

Bezoekers moet je altijd vooraf aanmelden bij de receptie, dat kan door een ticket aan te maken in de Self-service desk. Bezoekers moeten zich altijd aan- en afmelden bij de receptie in pand I. Bezoekers krijgen een bezoekerspas. Zo voorkomen we dat externe personen zomaar mee naar binnen lopen. Let erop dat je deze personen altijd begeleid binnen de ICS gebouwen. Breng ze ook altijd terug naar de receptie, zodat ze niet alleen door de panden lopen. Bezoekers moeten hun bezoekerspas zichtbaar dragen en bij vertrek weer persoonlijk inleveren bij de receptie.