Beleidslijn informatieveiligheid en privacy

Data veiligheid

(BLD DATA SEC)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

De snelle evolutie in de technologie voor digitale gegevensopslag en –transmissie doet het veiligheids- en privacy-risico enorm toenemen. Vooral doorgedreven miniaturisering en daardoor verhoogde mobiliteit vragen voor aangepaste maatregelen.

Door deze evolutie lijkt het aangewezen om een specifieke beleidslijn in te voeren afhankelijk van het type opslagmedium, de normaal verwachte mobiliteit en de mogelijkheid tot elektronisch verzenden van gegevens. Het feit of een digitaal opslagmedium al dan niet onderdeel uitmaakt van een intelligent apparaat heeft een invloed op de toepasbare informatieveiligheidsmaatregelen en dus op het geoorloofde gebruik. Bovenop een algemene beleidslijn kan het in bepaalde gevallen nodig zijn specifieke regels voor een bepaald type apparaat op te leggen.

Voor een verduidelijking betreffende het type van de gegevens (organisatiegegevens, persoonsgegevens, sociale gegevens, medische gegevens) wordt verwezen naar de beleidslijn data classificatie. De opslag, verwerking, transmissie van gegevens is niet toegelaten, tenzij onder toepassing van de regels in deze policy of expliciete autorisatie van de bevoegde dienst.

De beveiliging van gegevens wordt benaderd vanuit de gebruikte opslag en transmissietechnieken en beperkt zich tot algemene richtlijnen. In elk geval moeten de nodige maatregelen genomen worden om te voldoen aan de geldende wettelijke bepalingen, ondermeer voor opslag, toegang tot gegevens en geheimhouding . Het toepassingsgebied is op het vlak van technologie en op het vlak van apparatuur.

Dit document geeft uitleg over de maatregelen van toepassing op alle gegevens die de organisatie in het kader van haar missie gebruikt of die op haar infrastructuur gebruikt worden. Met andere woorden, op alle gegevens die binnen of buiten de organisatie, door haar of in haar naam opgeslagen worden op analoge of digitale opslagmedia (al dan niet haar eigendom), op enige wijze fysiek verplaatst worden of tussen eender welke opslagmedia op elektronische wijze uitgewisseld worden.

2. Data veiligheid

Elke organisatie onderschrijft de volgende beleidslijn van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

- Elke organisatie moet de toegang tot de gegevens[1] nodig voor de toepassing en de uitvoering van de sociale zekerheid beveiligen door middel van een identificatie-, authenticatie- en autorisatiesysteem.

1 In deze norm wordt onder de term “gegeven” niet enkel de sociale persoonsgegevens verstaan maar alle logische elementen van een informatiesysteem die voor de verwerking ervan instaan. Voorbeelden zijn: programma’s, toepassingen, bestanden, systeem utility’s en andere elementen van het besturingssysteem.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2007		V2007	Eerste versie	10/10/2007	10/10/2007
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de veiligheidsconsulent van het eHealth platform.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- NIST, SP800-60 volume II revision 1, “Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories”, Augustus 2008, 279 blz.

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- http://www.iso.org/iso/iso27001
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=68427
- http://www.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Bijlage C: Richtlijnen data veiligheid

A. Gegevens op analoge drager

Hieronder verstaan we de gegevens die op een digitale wijze opgeslagen zijn, meestal op papier.

1 Creatie

De drager moet voldoen aan de kwaliteitsvereisten die voor de toepassing redelijkerwijze mogen verwacht worden. Het aanmaken van gegevens gebeurt waar mogelijk vanaf een gevalideerde bron. Het aanmaken van gegevens moet in overeenstemming zijn met de geldende reglementering. Er moeten maatregelen genomen worden die zo nodig de authenticiteit van het document kunnen aantonen. In functie van informatieveiligheid moet het aanmaken van gegevens op analoge drager maximaal vermeden worden.

2 Opslag

Niet-publieke gegevens moeten minstens beveiligd zijn door een fysieke perimeter met toegangscontrole. Medische persoonsgegevens moeten minstens beveiligd zijn door een dubbele fysieke perimeter met toegangscontrole. Er moet een nominatieve lijst bestaan van alle personen die toegang hebben tot de kleinste perimeter met vermelding van hun specifieke bevoegdheden[2] . Op alle plaatsen waar originele documenten bewaard worden moeten adequate maatregelen genomen worden om verlies door omgevingsinvloeden tegen te gaan.

3 Verwerking

De verwerking van persoonsgegevens mag uitsluitend gebeuren door bevoegde personen. De verwerking van medische gegevens gebeurt – behoudens uitzonderingen - binnen een fysieke perimeter met toegangscontrole. Voor alle verwerkingen op medische gegevens moet een nominatieve lijst bestaan van alle personen die toegang hebben, met vermelding van hun specifieke bevoegdheden. Deze lijst staat onder toezicht van de verantwoordelijke geneesheer voor de verwerking van medische gegevens[3] . Het opvolgen van de verwerking moet op een gecontroleerde manier gebeuren.

4 Fysiek Transport

Voor transport van gegevens binnen de perimeter van een gebouw moeten geen specifieke beveiligingsmaatregelen genomen worden voor zover het transport steeds onder toezicht is van een bevoegde persoon. Transport van niet-publieke gegevens moet minstens beveiligd zijn door een fysieke perimeter en beheerd worden door een vertrouwde transporteur. Transport van medische persoonsgegevens moet minstens beveiligd zijn door een fysieke perimeter, beheerd door een eigen transportdienst. Indien geen eigen transport kan georganiseerd worden moet de beveiliging gebeuren met een verzegelde container en beheerd door een vertrouwde transporteur. In uitzonderlijke gevallen kan hiervan afgeweken worden mits toestemming van de verantwoordelijke geneesheer die bijkomende veiligheidsmaatregelen kan opleggen. Voor elk transport van medische persoonsgegevens buiten de fysieke perimeter moeten transportgegevens (wie, wat, wanneer) geregistreerd worden.

5 Vernietiging

De vernietiging van documenten die sociale persoonsgegevens bevatten moet op een gecontroleerde manier gebeuren. Vernietiging kan door versnippering, of door het verzamelen in speciale containers. De inhoud van deze containers wordt door een gespecialiseerde firma vernietigd. Vernietiging van originele gegevens kan uitsluitend met medeweten van de eigenaar en rekening houdend met de wettelijke bepalingen die erop van toepassing zijn. De actie van de vernietiging moet het voorwerp uitmaken van een autorisatie.

[2] Wet van 15 januari 1990 houdende oprichting van een kruispuntbank van de sociale zekerheid, art.26, §2

[3] Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.26, §1, §2

B. Digitale gegevens op de vaste infrastructuur

Hieronder verstaan we de digitale gegevens die opgeslagen zijn op vaste werkposten, servers en hun opslagsystemen. In uitbreiding ook de gegevens die uitsluitend via een vast bekabeld intern netwerk (LAN), dat aan de organisatie behoort, gecommuniceerd worden. Zodra een vaste werkpost fysiek verplaatst wordt zijn de richtlijnen voor mobiele apparatuur van toepassing. Wanneer opgeslagen gegevens op een andere wijze dan via het vaste netwerk getransporteerd worden zijn de richtlijnen voor elektronische communicatie van toepassing. De aangenomen hypothese bij deze opsplitsing is dat de vaste toestellen en het vaste netwerk afdoende beveiligd worden door een combinatie van hun fysieke perimeter, hun logische toegangscontrole en de genomen controlemaatregelen (logging, monitoring). In de context van elektronische transmissie en opslag kunnen vestigingen van de organisatie beschouwd worden als behorend tot hetzelfde vaste netwerk indien de onderlinge dataverbindingen een hoge graad van beveiliging hebben en de fysieke toegang in elk van deze gebouwen afdoende gecontroleerd is. Ongeautoriseerde apparatuur mag niet aan het vaste netwerk van de organisatie aangesloten worden. Het vaste netwerk moet zodanig beveiligd zijn dat het aansluiten van ongeoorloofde apparatuur opgespoord of verhinderd kan worden.

1 Creatie

De apparatuur moet voldoen aan de kwaliteitsvereisten die voor de toepassing redelijkerwijze mogen verwacht worden. Het aanmaken van gegevens gebeurt waar mogelijk vanaf een gevalideerde bron. Het aanmaken van gegevens moet in overeenstemming zijn met de geldende reglementering. Er moeten maatregelen genomen worden die zo nodig de authenticiteit van de gegevens kunnen aantonen.

2 Opslag

Niet publieke persoonsgegevens mogen niet op de vaste werkpost opgeslagen worden, tenzij voor de duur van een toepassingssessie. De systemen voor opslag van niet-publieke persoonsgegevens moeten minstens beveiligd zijn door een dubbele fysieke perimeter met toegangscontrole. Er moet een nominatieve lijst bestaan van alle personen die toegang hebben tot de kleinste perimeter met vermelding van hun specifieke bevoegdheden.

3 Verwerking

De logische toegang tot niet-publieke gegevens moet georganiseerd zijn via een systeem voor identificatie, authenticatie en autorisatie. Alle verwerkingen op deze gegevens kunnen uitsluitend gebeuren via werkposten die op het vaste netwerk van de organisatie aangesloten zijn. Verwerkingen vanaf of via een ander netwerk vallen onder de richtlijnen voor gegevensuitwisseling en/of mobiele opslagmedia. Voor alle verwerkingen op medische gegevens moet een nominatieve lijst bestaan van alle personen die toegang hebben, met vermelding van hun specifieke bevoegdheden. De verwerking van deze gegevens gebeurt onder toezicht van een verantwoordelijke geneesheer[4].

4 Transport

Fysiek transport van deze gegevens blijft alleen toegelaten onder controle van de bevoegde dienst voor informatica, en uitsluitend in het kader van hun rechtmatige bevoegdheden. Hiervoor gelden specifieke operationele richtlijnen. Elektronisch transport van deze gegevens is uitsluitend toegelaten over het vaste netwerk van de organisatie. Indien deze gegevens buiten het vaste netwerk van de organisatie verstuurd worden of op een andere wijze dan via dat vaste netwerk, dan gelden de specifieke richtlijnen voor gegevensuitwisseling.

5 Toelichting

De verschillende hoofdgebouwen en de regionale gebouwen vormen elk een aparte fysieke perimeter. Indien het netwerk tussen deze gebouwen een hoge graad van beveiliging heeft, kan het totale netwerk in en tussen deze gebouwen beschouwd worden als deel van hetzelfde vaste netwerk, voor zover de fysieke perimeter onder controle valt van de organisatie. Voor een mobiel apparaat dat door de bevoegde ICT dienst speciaal geconfigureerd werd om rechtstreeks op het vaste netwerk te worden aangesloten mag de aan- en afsluiting van het netwerk door de gebruiker zelf gebeuren. Voor beveiliging van de gegevens gelden de regels voor mobiele apparatuur. Het opslaan van niet-publieke gegevens vereist de fysieke perimeter van het gebouw en een tweede fysieke perimeter daarbinnen, bijvoorbeeld een computerzaal of een afgesloten lokaal. Het permanent opslaan van dergelijke gegevens op een vaste werkpost in een niet afgesloten lokaal is daarom niet toegelaten.

[4] Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.26, §1, §2

C. Gegevens op mobiele opslagmedia

Zowel digitale opslagmedia als apparaten waarin dergelijke opslagmedia geïntegreerd zijn of gebruikt kunnen worden en die niet permanent met het vaste netwerk verbonden zijn vallen onder deze rubriek (voorbeelden zijn laptop, smartphone, CD, DVD, verwisselbare harddisk, memory stick, flash geheugens, backup-media, cloud storage).

1 Algemeen

Elke uitwisseling van gegevens van of naar mobiele opslagmedia vallen onder de regels voor gegevensuitwisseling. Het gebruik van mobiele opslagmedia voor de verwerking van gegevens in het kader van de opdracht is uitsluitend toegestaan mits een expliciete autorisatie en met een welbepaald doeleinde. Het is niet toegestaan om mobiele opslagmedia direct te verbinden met het vaste netwerk van de organisatie, tenzij mits autorisatie door de bevoegde dienst. Het aansluiten van mobiele opslagmedia op apparatuur of op het netwerk van de organisatie en dit via eender welke methode, geeft de organisatie het recht om alle nodig geachte veiligheidsmaatregelen te nemen, inclusief het testen op virussen, het nemen van kopieën en onderzoek naar naleving van het interne reglement. Het gebruik van opslagmedia of apparatuur die niet aan de veiligheidsregels beantwoorden is niet toegelaten.

2 Opslag

De opslag van vertrouwelijke gegevens op mobiele apparatuur vereist het versleutelen van de gegevens[5], uitgezonderd voor het beperkt opslaan van persoonsgegevens waarvoor de privacywet een expliciete uitzondering voor verwerking voorziet[6]. Het opslaan van vertrouwelijke gegevens op mobiele opslagmedia of apparatuur is uitsluitend toegestaan na goedkeuring door de bevoegde dienst van de organisatie. Van alle gegevens die op mobiele opslagmedia opgeslagen worden moet regelmatig een backup gemaakt worden op het vaste netwerk.

3 Verwerking

Deze paragraaf is enkel van toepassing wanneer het mobiele apparaat voldoende intelligentie bevat waardoor gegevensverwerking mogelijk is. We spreken van online verwerking indien voor het verwerken van gegevens toegang vereist is tot het vaste netwerk en er daarvoor een verbinding moet worden opgezet. In alle andere gevallen betreft het een offline verwerking. Voor het overbrengen van gegevens van/naar het draagbare apparaat gelden bovendien de richtlijnen voor gegevensuitwisseling. Bij verwerking van vertrouwelijke gegevens neemt de gebruiker de nodige voorzorgen zodat derden geen inzage krijgen.

- Online verwerking : Een mobiel apparaat mag enkel rechtstreeks op het vaste netwerk aangesloten worden indien het daar specifiek voor geconfigureerd is; in alle andere gevallen van online verwerking moet de verbinding steeds verlopen via het extranet van de organisatie. Voor primaire organisaties betekent dit via het extranet van de sociale zekerheid. De toegang tot online gegevens zal, afhankelijk van hun classificatie, met een aangepast niveau en vorm van authenticatie gepaard gaan. De toegang tot vertrouwelijke gegevens op het vaste netwerk moet georganiseerd zijn via een nominatief systeem voor identificatie en autorisatie dat éénduidig zowel het apparaat als de gebruiker identificeert. Verwerking mag niet gebeuren op apparaten die deze functionaliteit niet ondersteunen. Er mogen geen andere, gelijktijdige verbindingen opgezet worden die de veiligheid van de online verwerking in gevaar kunnen brengen.
- Offline verwerking : Bij verwerking van gegevens offline is het de verantwoordelijkheid van de gebruiker om op regelmatige tijdstippen de gewijzigde gegevens te synchroniseren naar een online opslagmedium. Bij offline verwerking is het de verantwoordelijkheid van de gebruiker om op regelmatige tijdstippen de beveiligingssoftware te laten bijwerken.

4 Toelichting

Mobiele apparaten vallen onder strengere veiligheidsvereisten dan apparaten op het vaste netwerk. De richtlijnen voor mobiele apparaten blijven van toepassing, ook als de mobiele apparaten geconfigureerd zijn om op het vaste netwerk te worden aangesloten of er effectief op aangesloten zijn. Ook apparaten die geen eigendom zijn van de

[5] De KSZ vereist immers aangepaste maatregelen, volgens de Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.22, art.26, §3

[6] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, art.3, §2

organisatie kunnen in bepaalde gevallen gebruikt worden voor het verwerken van niet-vertrouwelijke gegevens, zoals het raadplegen van een website of e-mail via een thuis-PC.

D. Gegevensuitwisseling

1 Regels

Elke elektronische uitwisseling van gegevens tussen vaste en/of mobiele opslagmedia en apparaten vallen onder deze rubriek, van zodra minstens één van deze opslagmedia of apparaten eigendom is van de organisatie of in onderaanneming voor haar missie gebruikt wordt. Het uitwisselen van gegevens tussen toestellen die aangesloten zijn op het vaste netwerk van de organisatie werd behandeld in het hoofdstuk 'Digitale gegevens op de vaste infrastructuur'. Bij uitwisseling van vertrouwelijke gegevens moeten de bron en de bestemming van de gegevensoverdracht een vertrouwde partij zijn. Bij uitwisseling van persoonsgegevens is een wederzijdse authenticatie noodzakelijk. De uitwisseling van gegevens tussen een mobiel opslagmedium en het vaste netwerk moet te allen tijde controleerbaar zijn door de bevoegde dienst van de organisatie. De transmissie van vertrouwelijke gegevens dient steeds te gebeuren in versleutelde vorm. In principe volstaat versleuteling van het transmissiekanaal. Indien twijfels bestaan over de graad van beveiliging van het transmissiekanaal, dienen de gegevens zelf versleuteld te worden. Voor elke elektronische uitwisseling van gegevens moeten de geldende autorisaties en reglementering strikt gerespecteerd worden. Indien tussentijdse opslagruimtes buiten de controle van de organisatie vallen, moet erover gewaakt worden dat eventuele restanten van de transmissietrafiek versleuteld zijn. Medische gegevens moeten versleuteld worden vóór verzending, tenzij de transmissie gebeurt in een door de organisatie gecontroleerde end-to-end versleutelde verbinding.

2 Toelichting

Zodra gegevens het vaste netwerk verlaten (mobiel worden) zijn de richtlijnen voor gegevensuitwisseling van toepassing. Hierdoor valt ook het extern versturen en ontvangen van informatie via e-mail en internet onder deze richtlijn. Wanneer de organisatie vertrouwelijke informatie toegestuurd krijgt, zelfs via een onveilige weg, dan moet deze volgens de classificatie van de betreffende gegevens opgeslagen worden. Het zelf versturen van vertrouwelijke gegevens via deze kanalen zonder bijkomende veiligheidsmaatregelen is zonder meer verboden. Het lokaal synchroniseren van bvb agendagegevens is mogelijk voor zover er geen vertrouwelijke gegevens uitgewisseld worden.

Bijlage D: Data veiligheidsconcepten

1. Data Retentie

Een data retentie policy is een overeengekomen of opgelegd protocol dat bepaald hoelang gegevens (data) bewaard moeten blijven en toegankelijk moeten zijn, dit volgens de eventueel bestaande regel- en wetgeving of volgens business- of persoonlijke noodzakelijkheid.
De retentieperiode voor het bewaren van gegevens is afhankelijk van de aard van het document en van de wettelijke bepalingen die zijn vastgelegd om deze te bewaren.

Type data – Voorbeelden

Gebruikers- en applicatiedata

- Verslagen van vergaderingen (minutes)
- Contracten & licenties
- Verzekeringsdocumenten
- Personeelsgegevens
- Bedrijfsgegevens
- E-mail

Systeemdata

- Microsoft Windows
- Linux Red hat
- Oracle virtual machine (OVM)

Volgende beslissingen moeten worden genomen:
- Is de informatie bedrijf kritisch is; m.a.w. kan het bedrijf blijven verder bestaan zonder deze data?
- Is deze persoonsgebonden? Voldoet het behoud ervan aan de regelgeving betreffende privacy?
- Zijn er legale redenen om data bij te houden?
- Wanneer is data voor het laatst gebruikt? Is ze niet irrelevant?
- Wordt er geen dubbele data bijgehouden?
- Moet al die e-mail worden bewaard voor direct gebruik?

De vraag moet ook gesteld worden of informatie bedrijf kritisch is; m.a.w. kan het bedrijf blijven verder bestaan zonder deze data?
- Is data persoonsgebonden?
- Zijn er legale redenen om data bij te houden?
- Wanneer is de data voor het laatst gebruikt? Is ze niet irrelevant?
- Wordt er geen dubbele data bijgehouden?

Als er geen regelgeving is kan men stellen dat het bijhouden van data beperkt moet blijven tot de tijd die nodig is voor het verwezenlijken van de doelen waarvoor de gegevens verzameld werden.

Opmerking: Uit standpunt van informatieveiligheid dient de toegang tot gegevens beperkt te worden tot de eigenaar van de gegevens. Het is dus belangrijk van om de data goed te classificeren volgens belangrijkheid en eigenschappen en hieraan een bepaalde retentietijd aan te koppelen. Deze classificatie dient te gebeuren door elke sectie of departement dat verantwoordelijk is voor die documenten.

2. Data Back-up

Een back-up is een kopie van gegevens welke uit veiligheid wordt genomen ten einde corrupte of verdwenen data te kunnen herstellen in de oorspronkelijke staat.

Dezelfde classificatie i.v.m. het bepalen van de retentie is hier dus ook geldig. De retentietijd van een back-up kan echter verschillen van de retentietijd van de data welke zich op de verschillende apparaten bevinden. De toegang tot back-up is afhankelijk van de back-up procedures van de organisatie. Daarin wordt beschreven hoe een back-up wordt genomen en waar de verantwoordelijkheden liggen.

Opmerking: In de classificatietabel van de documenten kunnen dus volgend bijkomende parameters worden vermeld:
- Is een back-up wel nodig? Systeemdata?
- Moet al die e-mail wel bewaard worden en dus geback-upt?
- Retentietijd back-up?
- Behandeling van ROT-bestanden (Redundant, Overbodige of verOuderd, Triviale)?
- Moeten de gegevens geëncrypteerd worden? Hoe gaat dan het key-management uitgevoerd worden?
- Wie heeft toegang tot de back-up?
- Is het kritische data? RPO (Recovery point objective) /RTO (Recovery Time objective)

Om te vermijden dat onrealistische retentietijden worden gespecifieerd in de data analyse, dient men de verantwoordelijke er op te wijzen dat deze een impact heeft op de (interne) facturatie. Elke organisatie dient dus een back-up beleid op te stellen waarin alle deze details beschreven worden.

3. Data Archivering

Bij een archivering worden de oorspronkelijke gegevens verwijderd en weggeschreven naar een beveiligde omgeving waar de integriteit van de data niet kan worden aangetast.

Als de retentieperiode van de data verlopen is kan beslist worden om data te archiveren. Afhankelijk van het archiveringsprogramma kunnen dan verschillende handelingen plaatsvinden. Bij archivering wordt de data dan gekopieerd naar een andere locatie, eventueel omgezet naar een ‘open’ formaat, voorzien van een tijdstempel en

weggeschreven naar een - bij voorkeur - niet-vluchtig media, bijvoorbeeld wormtape of wormdisk.[7] Dit type media zorgt ervoor de gearchiveerde media niet meer kan worden gewijzigd om legale redenen. Het gebruik van een 'open' formaat zorgt ervoor dat de gearchiveerde data terug kan worden ingelezen in recentere versies van applicaties, of eventueel geïmporteerd in concurrerende programma's.

Opmerking: In de classificatietabel van de documenten voorzien we een aanduiding of data kan/mag gearchiveerd worden en indien ja, voor hoelang. Nadat de retentieperiode van de archivering verlopen is dient de fysische media door gespecialiseerde firma's te worden vernietigd.

4. Data Vernietiging

Het protocol bepaald ook hoe data op een effectieve manier daadwerkelijk kan of mag verwijderd worden, rekening houdende met de bestaande regel- en wetgeving of het overbodig worden van de gegevens.

Nadat de retentieperiode van de archivering verlopen is dient de fysische media door gespecialiseerde firma's te worden vernietigd.(Destroy). Andere data welke ergens op staat kan op verschillende manieren worden verwijderd:

- **A.** Clear: het softwarematig verwijderen van data, door standaard commando's of resetten naar fabrieksinstellingen, dit laatste is dikwijls de aanbevolen methode bij mobiele toestellen en routers/switches.
- **B.** Purge: hierbij worden labotechnieken toegepast of dat op fysische of logische wijze (crypto grafische technieken) te verwijderen van de media (shredder, demagnetisatie) – voor dit laatste is wel gespecialiseerde software nodig. Voor SSD-schijven bestaat er meestal een veiligheidsprocedure om de schijf te wissen. Deze is meestal eigen aan de fabrikant, waar men dan ook de juiste informatie kan vinden. (zoeken naar SSD secure erase utility). Ook voor SSD bestaat commerciële software om op een veilige manier te wissen, voorbeeld is: 'Parted Magic'.
- **C.** Destroy: de fysische vernietiging van de media – dient altijd te worden toegepast wanneer de media – bijvoorbeeld een harddisk defect is.
- **D.** Reïnstall: bij hergebruik van toestellen kan het voldoende een nieuwe image te installeren (type Ghost, Bare Metal), gezien deze de bestaande data volledig overschrijft.

Een bijzondere aandacht dient men te besteden aan toestellen die gebruikt worden onder het principe van BYOD (Bring Your Own Device). Hierbij kunnen privésystemen gekoppeld worden aan het netwerk van de organisatie. De zwakste schakel in de beveiliging is hier de gebruiker. Bij diefstal van onbeveiligde systemen wordt data blootgesteld aan zware risico's. Er bestaat software – eenmaal geactiveerd - die data van systemen kan onbruikbaar maakt eens die op het internet worden geconnecteerd. Dezelfde principes zijn geldig bij telewerken en verplaatsingen buiten de organisatie. Een goede fysische bescherming dient gepromoot te worden bij de gebruiker

5. Data Audit

Op regelmatige basis dient een audit te gebeuren om te controleren of de back-uppolicy en de classificatie van gegevens up-to-date is en of deze daadwerkelijk werd toegepast. De data audit wordt uitgevoerd door een persoon niet-eigen aan de dienst welke instaat voor het beheer van de gegevens. Deze data audit resulteert in een rapport dat besproken wordt met de verantwoordelijk van de organisatie om te nemen acties te bepalen. Naderhand wordt een nieuwe audit uitgevoerd om te controleren of de gevraagde aanpassingen wel degelijk werden uitgevoerd.
Om deze data audit uit te voeren dient een audit-document (checklist) te worden opgesteld door elke organisatie welke afgestemd is op hun beleidslijnen en classificaties.

6. Data Incidenten

De gegevens worden beveiligd met de juiste credentials. Het is echter noodzakelijk om een procedure te voorzien waarbij inbreuken op de informatieveiligheid – vrijwillig of niet – gesanctioneerd worden, gezien het lekken van informatie zware bedrijfs- en/of imagoschade kunnen veroorzaken.
Een voorbeeld van dergelijke incident is het meenemen van media door firma's die het onderhoud onder garantie uitvoeren op bijvoorbeeld storage, disks, servers; dit is een inbreuk op de informatieveiligheid en zou uitdrukkelijk contractueel moeten worden vastgelegd dat dit niet mag.

[7] WORM: Write Once Read Many times

Deze procedure moet door elke organisatie te worden opgesteld, gezien een inbreuk niet voor elke organisatie even zwaar doorweegt. Er moet ook worden voorzien dat media niet door externe bedrijven mag worden meegenomen.

7. Uitzonderingen

Op elke regel zijn uitzonderingen. Niet altijd kan data op een standaard wijze behandeld worden, omwille van bijvoorbeeld technische beperkingen van apparatuur, tekort aan storage, of om confidentiële redenen. Of het nu permanent of tijdelijk is, het classificatiemodel is de ideale plaats om de uitzonderingsituatie te vermelden. Wanneer uitzonderingen niet geregistreerd worden loopt men anders immers het risico dat de uitzondering 'vergeten' wordt, wat op termijn kan leiden tot vervelende situaties. Het blijft de persoon die de classificatie documenten opstelt zijn verantwoordelijkheid dat deze uitzonderingen worden geregistreerd.

Bijlage E: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	
Veilig personeel	
Beheer van bedrijfsmiddelen	**Ja**
Toegangsbeveiliging	
Cryptografie	**Ja**
Fysieke beveiliging en beveiliging van de omgeving	**Ja**
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	**Ja**

***** EINDE VAN DIT DOCUMENT *****