Universitair Informatiemanagement

UNIVERSITEIT TWENTE.

Kenmerk: SECR/IM/11/0412/khv
Datum: 21 september 2011

Classificatierichtlijn Informatie en Informatiesystemen Universiteit Twente

Gebaseerd op de Modelvragenlijsten voor de Classificatie van Informatie en Informatiesystemen van SURFibo van juli 2010.

1 Inleiding

Deze classificatierichtlijn werkt de classificatie van Informatie en Informatiesystemen uit zoals beschreven in het Informatiebeveiligingsbeleid Universiteit Twente. Deze richtlijn is zo geschreven dat zij bruikbaar is tijdens het classificatieproces zonder dat het Informatie-beveiligingsbeleid Universiteit Twente geraadpleegd hoeft te worden.

1.1 Algemeen

Bij de Universiteit Twente wordt gewerkt met informatie en geautomatiseerde informatie-systemen. Aandacht voor de beveiliging van informatie is noodzakelijk. Het gaat daarbij om de juiste mate van beveiliging, één die past bij de risico's die de informatie loopt. Classificatie van informatie geeft een inschatting van de gevoeligheid en het belang van de informatie en de daarbij horende graad van beveiliging. Classificatie levert zodoende een bijdrage aan het bepalen van de juiste mate van beveiliging van de informatie.

Zoals beschreven in het Informatiebeveiligingsbeleid Universiteit Twente dient de classificatie door of namens de eigenaar van het betreffende informatiesysteem te worden bepaald. Voor de instelingssystemen van de UT zijn door het College van Bestuur houders (directeuren van diensten) aangewezen die de rol van eigenaar vervullen.

1.2 Reikwijdte

Het classificatiesysteem bij de Universiteit Twente heeft zowel betrekking op informatie (data/gegevens), als op de systemen waarin deze informatie is opgeslagen (informatiesystemen).

Classificatie betreft alle, zowel centrale als decentrale, informatie(systemen), waarop het informatiebeveiligingsbeleid van de Universiteit Twente van toepassing is.

1.3 Doelstelling Classificatie

Voor het goed functioneren van de Universiteit Twente is het omgaan met informatie van levensbelang. Bedrijfsvoering, studenten en medewerkers moeten er op kunnen vertrouwen dat informatie toegankelijk is wanneer ze nodig is, correct en volledig is en alleen beschikbaar is voor daartoe geautoriseerde personen.

Niet alle informatie is vertrouwelijk. Dus is het niet erg gebruiksvriendelijk om niet vertrouwelijke informatie net zo streng te beschermen als hoog vertrouwelijke informatie. Proportionaliteit, ook omwille van efficiënt gebruik van de beschikbare financiële middelen, is hierbij gewenst. Het ligt voor de hand om onderscheid in bescherming aan te brengen. Classificatie is hiervoor het hulpmiddel.

2 Uitgangspunten en kaders

2.1 Uitgangspunten

Bij de Universiteit Twente gelden de volgende uitgangspunten voor classificatie van informatie en informatiesystemen:

1. De baseline informatiebeveiliging wordt overal toegepast, dit zijn de minimaal voorgeschreven beveiligingsmaatregelen;
2. Waar uit de risicoanalyse blijkt dat additionele maatregelen noodzakelijk zijn, dienen deze getroffen te worden;
3. Het geheel aan informatiebeveiligingsbeleid en -maatregelen wordt periodiek onderworpen aan een audit;
4. Op basis van de auditresultaten worden nieuwe jaarplannen voor informatiebeveiliging opgesteld;
5. De uitvoering van de classificatie gebeurt onder de verantwoordelijkheid van de houder van het informatiesysteem.

2.2 Kaders met betrekking tot betrouwbaarheid

Hieronder een korte bespreking van de kaders die een rol spelen bij de bevordering van de betrouwbaarheid van informatie. Het gaat daarbij om de begrippen Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

Beschikbaarheid

Onder *beschikbaarheid* wordt bij de Universiteit Twente verstaan: het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante voorzieningen.

Elementen die beschikbaarheid bepalen zijn bijvoorbeeld een betrouwbare stroomvoorziening, adequate brandbeveiliging, de aanwezigheid van een actueel continuïteitsplan, betrouwbare reservekopieën en het ontbreken van zogeheten ‘single points of failure’. Andere belangrijke aspecten zijn het bestaan van voldoende toegangsmogelijkheden voor het beoogde aantal gelijktijdige gebruikers en bescherming tegen zogeheten ‘denial of service’-aanvallen.

Integriteit

Onder *integriteit* wordt bij de Universiteit Twente verstaan: het waarborgen van de correctheid en de volledigheid van informatie en verwerking.

Elementen van integriteit zijn bijvoorbeeld het aanbrengen van wijzigingen door geautoriseerde personen, geldigheidscontroles en het registreren van wijzigingen.

Vertrouwelijkheid

Onder *vertrouwelijkheid* wordt bij de Universiteit Twente verstaan: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Elementen van vertrouwelijkheid zijn bijvoorbeeld versleuteling van informatie (encryptie) en authenticatie van de gebruiker zodra deze zich toegang tot de gegevens wil verschaffen.

2.3 Klasse-indeling voor informatie

De onderstaande klasse-indeling, wordt bij de Universiteit Twente gebruikt voor elk van de BIV kaders:

Beveiligingsklasse 'standaard'

De classificatie *standaard* betekent bij de Universiteit Twente dat het betreffende systeem voor het/de betreffende kader(s) moet voldoen aan de minimale eisen die aan alle ICT-voorzieningen gesteld worden. Het pakket aan standaard beveiligingsmaatregelen wordt ook wel de "baseline beveiliging" genoemd en is het geheel van maatregelen dat bij de Universiteit Twente overal getroffen moet worden ook al geeft de classificatie geen aanleiding tot extra maatregelen.

Als een systeem de classificatie *standaard* krijgt, betekent dit dus dat alle standaard beveiligingsmaatregelen voor de BIV-aspecten, die voor dit systeem relevant zijn, moeten worden geïmplementeerd.

Beveiligingsklasse 'gevoelig'

De classificatie *gevoelig* betekent dat een inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie een verstoring veroorzaakt in een van de primaire processen, maar niet van zeer ernstige of onomkeerbare aard. Ook mogelijke negatieve effecten voor het imago van de Universiteit Twente kunnen aanleiding zijn om een classificatie *gevoelig* toe te kennen.

Voor systemen met de classificatie *gevoelig* op een of meerdere van de BIV-kaders zal ten opzichte van de "baseline beveiliging" een aanvullend pakket beveiligingsmaatregelen voorgeschreven worden. De classificatie *gevoelig* brengt dus extra verplichtingen en dus extra kosten met zich mee. De maatregelen zullen doorgaans nog een algemeen, gestandaardiseerd karakter hebben, waarbij de kosten tot uiting kunnen komen als extra kosten in de dienstverleningsovereenkomst.

Beveiligingsklasse 'kritiek'

De classificatie *kritiek* wordt gereserveerd voor die systemen waarbij aantasting van beschikbaarheid, integriteit en vertrouwelijkheid een zeer ernstige of onomkeerbare verstoring van een van de primaire processen veroorzaken, ernstige schade toebrengt aan het imago van de Universiteit Twente of een wetsovertreding inhoudt.

Voor systemen met een classificatie *kritiek* op een of meerdere van de BIV-kaders geldt dat bovenop de maatregelen voor systemen met de classificatie *gevoelig* extra maatregelen getroffen dienen te worden. Dit kunnen weer gestandaardiseerde maatregelen zijn, maar er kan ook een vorm van maatwerk plaatsvinden.

3 Het Classificatieproces

De eigenaar van de Informatie en het Informatiesysteem is verantwoordelijk voor de uitvoering en het resultaat van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt ondersteund door een aantal vragenlijsten, waarmee de business impact wordt bepaald:

- Algemene vragen
- Vragen over beschikbaarheid
- Vragen over integriteit
- Vragen over vertrouwelijkheid

De business impact wordt beoordeeld op een 5-puntschaal:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de instelling

Vanuit de business impact beoordelingen kan een vertaling gemaakt worden naar de 3-puntschaal die gebruikt wordt voor de BIV classificatie.

Voor de classificatie naar de inzichten **integriteit** en **vertrouwelijkheid** kan die vertaling als volgt zijn:

Business impact	**I of V classificatie**
1 + 2	Standaard
3	Gevoelig
4 + 5	Kritiek

Voor de **beschikbaarheid** is deze verdeling niet zo direct te leggen, maar de business impact beoordeling die daar uit komt geeft over het algemeen voldoende aanknopingspunten om een classificatie naar kritiek, gevoelig en standaard te maken.

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door of namens de eigenaar van het betreffende informatiesysteem te worden bepaald. Voor de instelingssystemen van de UT zijn door het College van Bestuur houders (directeuren van diensten) aangewezen die de rol van eigenaar vervullen.

Bij de uitvoering van het classificatieproces wordt de houder ondersteund door de Information Security Officer (UIM), functioneel beheerder (houder), applicatiebeheerder (ICTS/ISA) en zo nodig technisch beheerder.

De te gebruiken vragenlijsten zijn te vinden in Bijlage I. Om redenen van reproduceerbaarheid, bijvoorbeeld als audit-partijen om achtergrondgegevens vragen, en om vergelijking mogelijk te maken bij toekomstige herclassificatie, wordt de houder geadviseerd om de ingevulde vragenlijsten voor toekomstige referentie te archiveren.

4 Maatregelen

Het resultaat van de classificatie wordt bij de Universiteit Twente per BIV-aspect bepaald. De basis hiervoor zijn de ingevulde vragenlijsten. Op grond van de Business Impact kan voor alle drie aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid een classificatie Standaard, Gevoelig of Kritiek vastgesteld worden. Wanneer het bij de vragenlijsten voor B, I en V éénmaal voorkomt dat de hoogste beveiligingsklasse wordt gescoord, bepaalt dit doorgaans de klasse voor het gehele betreffende beveiligingsaspect. Daarmee dienen alle maatregelen behorende bij die klasse van dat aspect geïmplementeerd te worden. Hiervan kan door de houder worden afgeweken, doch uitsluitend voorzien van onderbouwde argumentatie.

De houder accepteert hiermee de verantwoordelijkheid voor de extra beveiligingsrisico's en de eventuele optredende gevolgen.

Wat betreft de te nemen maatregelen levert dit onderstaande tabel op:

	B	**I**	**V**
Standaard	SB	SI	SV
Gevoelig	SB + GB	SI + GI	SV + GV
Kritiek	SB + GB + KB	SI + GI + KI	SV + GV + KV

SB = standaardmaatregelen voor aspect B = de baseline voor aspect B
SI = standaardmaatregelen voor aspect I = de baseline voor aspect I
SV = standaardmaatregelen voor aspect V = de baseline voor aspect V
GB = extra maatregelen voor de klasse Gevoelig voor aspect B
GI = extra maatregelen voor de klasse Gevoelig voor aspect I
GV = extra maatregelen voor de klasse Gevoelig voor aspect V
KB = extra maatregelen voor de klasse Kritiek voor aspect B
KI = extra maatregelen voor de klasse Kritiek voor aspect I
KV = extra maatregelen voor de klasse Kritiek voor aspect V

Op basis van auditresultaten, technische ontwikkelingen en nieuwe inzichten zullen de geadviseerde maatregelen periodiek worden aangepast.

4.1 Uitwerking maatregelen

Om niet voor elk informatiebedrijfsmiddel opnieuw de exercitie te hoeven doen welke maatregelen getroffen moeten worden is er een matrix gedefinieerd waarin iedere classificatie automatisch gekoppeld wordt aan een set maatregelen.

Deze maatregelen zijn op hoofdlijnen gedefinieerd en laten ruimte als het gaat om de gedetailleerde invulling. Een deel van de hier gedefinieerde maatregelen is al operationeel. Een deel echter nog niet. De classificatie van de belangrijkste instellingssystemen zal mede de prioriteit in de implementatie van maatregelen bepalen.

Hoewel veel maatregelen technisch van aard zijn dient niet uit het oog verloren te worden dat de wijze waarop gebruikers omgaan met informatie minstens zo belangrijk, zo niet belangrijker is dan de technische maatregelen die we kunnen treffen. Tegen onverantwoord gedrag van gebruikers is geen technische maatregel opgewassen.

Kl.	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Kritiek	• Redundantie: Fail-over • Back-up: daily incremental, wekelijks full • Capaciteitsplanning middels geautomatiseerde trendwatching (dagelijkse controle) • Storingsdienst: 7x24	• Synchronisatie: real time • Correctie van fouten: direct na constatering • Autorisatie: op mutatie • Servercertificaten / SSL • Training alle gebruikers • Periodieke controle proces/data • Gebruik van digitale handtekening bij communicatie	• Encryptie van opslag • Veilige printomgeving • Informatie mag niet zonder uitdrukkelijke toestemming van de houder in geprinte vorm de gebouwen van de Universiteit Twente verlaten • Voor testdoeleinden mag geen kopie van de productiedata gebruikt worden
Gevoelig	• Noodstroomvoorziening • Redundantie: Cold standby • Back-up: daily incremental, maandelijks full • Continuïteitsplan / calamiteitenplan aanwezig • Capaciteitsplanning middels geautomatiseerde trendwatching (wekelijkse controle) • Ondersteuning: openstelling Universiteit • Onderhoud: buiten kantooruren	• Synchronisatie: binnen 1 werkdag • Correctie van fouten: binnen 1 werkdag • Autorisatie: op rol • Audittrail op mutatie/gebruiker • Inputvalidatie (serverside) • Functiescheiding • Zoveel mogelijk gebruik maken van servercertificaten, wanneer via het publieke netwerk benaderbaar dan verplicht toepassen van servercertificaten/ SSL. • Training (kern)gebruikers • Versiebeheer voor documenten, incl. timestamping • Authenticatie: intern via persoongebonden gebruikersnaam/wachtwoord, extern sterke authenticatie (2-factor authenticatie) indien mutatierechten	• Authenticatie: intern via persoongebonden gebruikersnaam/wachtwoord, extern sterke authenticatie (2-factor authenticatie) • Autorisatie naar rol • Niet via het publieke netwerk benaderbaar • Informatie is logisch niet in de DMZ geplaatst • Encryptie van datatransport • Audittrail • Encryptie van dataopslag op mobiele devices (notebook, USB) • Gecontroleerde afvoer (zowel papier als digitaal) • Clear desk • Voor gegevens die vallen onder de WBP is doelomschrijving, grondslag voor verwerking en indien van toepassing de privacytoets, de instemming van de URaad en de melding aan het CBP vastgelegd. • Distributie van gegevens alleen met toestemming van de houder. • Indien voor test doeleinden een kopie van de productiedata gebruikt wordt dan geldt hiervoor eenzelfde vertrouwelijkheidregime als voor de productiedata
Standaard	• Brondata staat centraal • Redundantie: Spares • Back-up: maandelijks calamiteiten • Capaciteitsplanning middels geautomatiseerde trendwatching (maandelijkse controle) • Ondersteuning: openstelling servicedesk • Onderhoud: In overleg met houder	• Voorkomen van schaduw bestanden • Correctie van fouten: binnen afgesproken tijd • Autorisatie: op groep • Authenticatie via persoonsgebonden gebruikersnaam/wachtwoord	• Authenticatie via persoonsgebonden gebruikersnaam/wachtwoord • Sterk wachtwoordbeleid (min. 8 posities, geen woorden of namen, opgebouwd uit cijfers, hoofd- en kleine letters) • Wachtwoorden worden via een veilige versleutelde verbinding verstuurd

De toelichting op de maatregelen is te vinden in Bijlage II.

5 Implementatie

Zoals beschreven in het Projectplan Verbeteringen Informatiebeveiligingsbeleid 2011 wordt in het najaar van 2011 de classificatie van de instellingssystemen gestart onder verantwoordelijkheid van de houder en ondersteuning vanuit UIM.

Na afronding van de classificaties van de instellingssystemen krijgen in 2012 de eigenaren/houders van de overige systemen het zelfde aanbod.

Bij nieuwe systemen wordt bij de start van het project de classificatie uitgevoerd.

Bijlage I: Vragenlijsten

Deze bijlage kan als invuldocument gebruikt worden en als basis dienen om de classificaties vast te stellen. Vul onderstaande gegevens in.

Documenteigenaar	
Functie	
Organisatieonderdeel	
Telefoonnummer	
Laatste datum invullen	

I.1 Algemeen

1. Gangbare naamsaanduiding en korte omschrijving van de ICT-voorziening
2. Voor welk(e) functionele doel(en) wordt de ICT-voorziening gebruikt?
   Denk aan hoofdfuncties, zoals administratie, onderwijs, publieksinformatie, etc. En aan doelgroepen van gebruikers
3. Welke gegevens worden vastgelegd in de ICT-voorziening?
   Denk aan structuur (teksten, tabellen, plaatjes) en inhoud (meetresultaten, personalia, locaties, financiën) e.d.
4. Worden in of vanuit de ICT-voorziening historische gegevens vastgelegd, dan wel periodiek weggeschreven naar andere media?
   Bedoeld is hier een interne en/of externe archiveringsfunctie en de regelmaat waarmee dit gebeurt, dus niet de reguliere back-up-functie.
5. Hoe lang worden gegevens online bewaard (nadat ze bedrijfsmatig zijn afgehandeld)?
   Denk aan afgegeven diploma's, promoties, pensioengegevens, enz. Specificeer de termijnen, bijvoorbeeld na een jaarafsluiting of na de diploma-uitreiking of pensionering
6. Vindt het transport van authenticatiegegevens plaats van en naar de ICT-voorziening?
   Zijn er client/server-verbindingen of webinterfaces? Met welke communicatie-protocollen?
7. Hoeveel personen in welke functies hebben mutatiebevoegdheid voor de ICT-voorziening?
   Maak hierbij onderscheid: autorisatie van gebruikers, mutatie van systeemtabellen, invoer van transacties, e.d.
8. Hoeveel personen in welke functies hebben raadpleegbevoegdheid tot de ICT-voorziening?
   Maak hierbij onderscheid: algemene raadpleegfunctie of persoonlijke gegevens van de gebruiker zelf, e.d.
9. Fungeert de ICT-voorziening als bronsysteem voor andere systemen d.w.z. worden gegevens(bestanden) verstrekt aan andere systemen?
   Specificeer per afnemend systeem de naamsaanduiding en de systeemhouder.
10. Is deze ICT-voorziening het enige in zijn soort voor de Universiteit Twente?
    Vermeld hier eventuele alternatieven (pakket, systeem, netwerkcomponent, e.d.)
11. Welke typen werkplekken zijn er voor raadpleging en/of mutatie van gegevens beschikbaar?
    Vermeld hier de mogelijkheden voor kantoor, thuis/internet en mobiel.
12. Voor wie is dit systeem van belang?
    Te denken valt aan Organisatie als geheel, Proceseigenaar, Gebruikers/proces-medewerkers, Geregistreerden (klanten, studenten, personeel, leveranciers, …)

I.2 Beschikbaarheid

In het kader van beschikbaarheid is het goed te kijken naar hoe groot de schade is die ontstaat bij een bepaalde uitvalsduur.

1. Welke groep gebruikers wordt getroffen door uitval van het informatiebedrijfsmiddel? En hoe groot is die groep? Wat is naar schatting het aantal gelijktijdige gebruikers in het informatiebedrijfsmiddel?
2. Wat moeten de openstellingstijden voor het informatiebedrijfsmiddel zijn? Welk beschikbaarheidspercentage is dan wenselijk?
3. Welke frequentie van systeemuitval wordt nog als acceptabel ervaren? (per maand / kwartaal / jaar)
4. Is er met ICTS een Service Level Agreement (SLA) afgesproken?
5. Is er een continuïteitsplan voor het informatiebedrijfsmiddel?
6. Is er sprake van kritieke uitval momenten? (denk bijv. aan salarisadministratie aan het eind van de maand, peildatum rapportages)
7. Maximaal toegestane downtime?

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de instelling

Business consequentie	**Business impact**				
Bij een uitvalsduur van	uur	dag	2-3 dagen	week	maand
Management beslissingen Hoe schadelijk is het als op basis van het niet beschikbaar zijn van informatie verkeerde management beslissingen worden genomen?					
Direct omzetverlies Verliezen we business / omzet als informatie niet beschikbaar is?					
Publiek vertrouwen Wordt het vertrouwen geschaad of is er imagoschade als informatiebedrijfsmiddel niet beschikbaar is?					
Extra kosten Moeten er extra kosten gemaakt worden als het informatiebedrijfsmiddel niet beschikbaar is?					
Aansprakelijkheid Kan het niet beschikbaar zijn van een applicatie leiden tot enige vorm van aansprakelijkheid?					
Recovery Wat kost het om de achterstand in werk weer weg te werken na een herstart?					
Medewerkers moreel Heeft het nadelige effecten voor het moreel of de motivatie van gebruikers als de applicatie niet beschikbaar is?					
Fraude Kan niet beschikbaar zijn van informatiebedrijfsmiddel leiden tot frauduleuze handelingen?					
Totaal score In samenvatting: wat is de meest ernstige schade die kan optreden bij uitval op het meest kritische moment?					

I.3 Integriteit

In het kader van integriteit is het van belang te beoordelen wat de gevolgen kunnen zijn van fouten in gegevens. Dit geldt zowel voor opzettelijke fouten (of fraude) als onopzettelijke fouten.

Gaat het bij vertrouwelijkheid om de vraag of een ander het gegeven mag zien, bij integriteit gaat het erom of de ander het gegeven mag muteren. Kernbegrippen zijn juistheid en volledigheid.

1. Vormen de gegevens in het informatiemiddel de basis voor management beslissingen?
2. Welke bewaartermijnen zijn van toepassing? (archiefwet, WBP, fiscale wetgeving, …)
3. Wordt er systematisch gecontroleerd op juistheid en volledigheid?
4. Vanaf welk soort werkplekken moeten gegevens beschikbaar zijn? (altijd en overal, thuis, onderwijslokalen, personeelswerkplek)
5. Kan een gebruiker onrechtmatig voordeel behalen door een gegeven opzettelijk te veranderen? (fraude te plegen)
6. Maximaal toegestaan dataverlies na uitval?

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de instelling

Business consequentie	**Business impact**				
	1	**2**	**3**	**4**	**5**
Management beslissingen Hoe schadelijk is het als op basis van deze informatie verkeerde management beslissingen worden genomen?					
Direct omzetverlies Verliezen we business / omzet als informatie ongeautoriseerd gewijzigd wordt?					
Publiek vertrouwen Hoe groot is de imagoschade als onjuiste informatie wordt gebruikt?					
Aansprakelijkheid Kan onjuistheid van gegevens leiden tot enige vorm van aansprakelijkheid?					
Medewerkers moreel Heeft het nadelige effecten voor het moreel of de motivatie van gebruikers als ze met onjuiste informatie moeten werken?					
Fraude Welke impact hebben frauduleuze handelingen?					
Totaal score In samenvatting: gegeven de bovenstaande scores (en eventueel andere consequenties) wat is dan de grootste schade die kan ontstaan door fouten of ongeautoriseerde wijzigingen? (dit zou normaal minimaal gelijk moeten zijn aan de grootste schade op individuele basis)					

I.4 Vertrouwelijkheid

Om te bepalen óf en hoe vertrouwelijk informatie is, is het van belang te weten wat de business consequenties zijn van ongeplande of ongeautoriseerde openbaarmaking of bekend worden van die informatie. Een speciale categorie vertrouwelijke gegevens zijn de persoonsgegevens. Bij de verwerking hiervan hebben we ons te houden aan de Wet Bescherming

Persoonsgegevens. Deze laat veel toe maar stelt wel voorwaarden aan de verwerking en dan vooral aan de zorgvuldigheid van omgang met die gegevens.

1. Worden in het informatiebedrijfsmiddel gegevens opgeslagen of verwerkt welke herleidbaar zijn tot natuurlijke personen?
2. Bevat het informatiebedrijfsmiddel informatie die gecombineerd met informatie uit andere systemen herleidbaar is tot natuurlijke personen?
3. Bevat het informatiebedrijfsmiddel concurrentiegevoelige gegevens (bijv. tarievenopbouw, contracten)?
4. Bevat het informatiebedrijfsmiddel informatie onder embargo?
5. Bevat het informatiemiddel informatie die alleen voor een specifieke doelgroep beschikbaar mag zijn? (denk ook aan licentiebeperkingen)
6. Bevat het informatiebedrijfsmiddel gegevens die gebruikt kunnen worden om fraude te plegen? (denk bijv. aan identiteitsfraude, creditcardnummers, wachtwoordbestanden).

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de instelling

Business consequentie	**Business impact**				
	1	**2**	**3**	**4**	**5**
Concurrentie nadeel Hoe schadelijk is het als informatie bij de concurrent terecht komt?					
Direct omzetverlies Verliezen we business / omzet als informatie in verkeerde handen terecht komt?					
Publiek vertrouwen Hoe groot is de imagoschade als deze informatie publiek wordt, hoe groot zijn de nadelige gevolgen voor het vertrouwen dat onze klanten in ons hebben?					
Aansprakelijkheid Kan openbaar maken leiden tot aansprakelijkheidstelling op basis van wettelijke of contractuele verplichtingen?					
Medewerkers moreel Heeft openbaarmaking nadelige effecten op het moreel of de motivatie van medewerkers?					
Fraude Welke impact hebben frauduleuze handelingen t.g.v. bekend worden van deze gegevens?					
Totaal score In samenvatting: gegeven de bovenstaande scores (en eventueel andere consequenties) wat is dan de grootste schade die kan ontstaan door het onbedoeld of ongeautoriseerde toegang bieden tot deze informatie? (dit zou normaal minimaal gelijk moeten zijn aan de grootste schade op individuele basis)					

Bijlage II: Toelichting op de maatregelen

II.1 Toelichting op maatregelen beschikbaarheid

Onderhoud: Is te plannen. Het gaat hier dus om het niet beschikbaar zijn van een systeem op een vooraf gepland tijdstip. Dit tijdstip dient altijd in overleg met de houder te worden vastgesteld. Voor informatiebedrijfsmiddelen die hierop gevoelig of kritiek scoren dient dit buiten kantooruren plaats te vinden.

Ondersteuning: Heeft betrekking op het in de lucht houden van het informatiebedrijfsmiddel inclusief het kunnen beantwoorden van vragen van gebruikers daarover. Openstelling van de servicedesk is gedurende kantooruren, openstelling van de Universiteit is ook 's avonds en op zaterdag. *(kunnen we dat zo stellen?)*

Storingdienst: Zorgt er voor dat een systeem in de lucht blijft maar beantwoord geen vragen van gebruikers.

Back-up: Reserve kopie. De frequentie waarmee deze gemaakt wordt is mede bepalend voor de snelheid waarmee deze, in geval van een calamiteit, terug gezet kan worden (restoren). Een incremental back-up maakt alleen een kopie van de wijzigingen t.o.v. de laatste back-up. Bij een restore moet de laatste full back-up en alle volgende incremental back-ups terug gezet worden.

Capaciteitsplanning: Capaciteitsplanning moet tijdig inzicht verschaffen in bijvoorbeeld het vol raken van schijven en cruciale bestanden (logfiles) en performance problemen voorkomen. Als schijven of specifieke bestanden "vol" raken kan dit betekenen dat een systeem ermee ophoudt. Te veel gebruikers op een systeem kan traagheid veroorzaken als gevolg van bijvoorbeeld geheugen problemen.

Redundantie: Is dubbele uitvoer van informatiebedrijfsmiddelen om ervoor te zorgen dat je bij defecten snel door kunt werken. *Spares* zijn reserve onderdelen zoals een reserve pc die uit het magazijn gehaald wordt en nog geïnstalleerd moet worden ter vervanging van een werkstation dat defect is op een werkplek. *Cold standby* betekent dat er een tweede systeem al volledig geïnstalleerd klaar staat maar er nog wel een menselijke handeling nodig is om deze aan te zetten. *Fail-over* is een techniek waarbij de functie van het systeem bij defect automatisch (dus zonder tussenkomst van mensen) over genomen wordt door een ander systeem. De gebruiker merkt hier (meestal) niets van.

Brondata centraal: Centraal maakt dat je ook back-up faciliteiten centraal geregeld kan hebben. Bij lokale opslag is dit aan de individuele gebruiker.

Continuïteitsplannen/ calamiteitenplannen: Een continuïteitsplan regelt vooral de beschikbaarheid van bedrijfsmiddelen en bedrijfsprocessen. Het zorgt dat er maatregelen zijn getroffen om processen snel te kunnen hervatten in geval van een calamiteit. Ook geeft het prioriteiten aan: welk bedrijfsmiddel en –proces heeft voorrang? Een calamiteitenplan beschrijft de acties die uitgevoerd moeten worden op het moment van een calamiteit. Het bevat doorgaans een escalatieplan en een uitwijkplan.

Noodstroomvoorziening: Zorgt ervoor dat systemen niet uitvallen in geval van een stroomstoring. Een stroomstoring op systemen die niet aangesloten zijn op een noodstroomvoorziening kunnen gevolgen hebben voor de integriteit van de gegevens op die systemen. Ook de snelheid waarmee deze systemen weer in de lucht gebracht kunnen worden wordt hier nadelig door beïnvloed. Er moet immers van alles gecontroleerd worden voordat zo'n systeem weer voor productie vrijgegeven kan worden.

II.2 Toelichting op maatregelen integriteit

Synchronisatie: Integriteit van data betekent dat wanneer data op verschillende plaatsen in de organisatie gebruikt wordt (vaak in verschillende systemen) men er van uit moeten kunnen gaan dat deze data ook hetzelfde is. Dit betekent in z'n algemeenheid dat je schaduwbestanden

(bv een telefoonlijstje in excel terwijl contactgegevens ook op het portaal staan) zoveel mogelijk moet voorkomen. Soms ontkom je er echter niet aan dat data op twee plaatsen wordt vastgelegd en gebruikt. Hier is het belangrijk dat er één bron systeem wordt aangewezen en er dus afspraken zijn gemaakt met welke frequentie de daarvan afhankelijke systemen een update van deze data ontvangen (= synchronisatie). Bij informatiebedrijfsmiddelen die de classificatie kritiek hebben meegekregen wordt real-time synchronisatie als eis gesteld wat betekent dat verandering in de brondata direct doorgevoerd moeten worden in dit afhankelijke bedrijfsmiddel.

Correctie van fouten: Afhankelijk van de classificatie van het informatiebedrijfsmiddel zal de snelheid waarmee correcties n.a.v. geconstateerde fouten doorgevoerd moeten worden verschillen.

Autorisatie: Middels de autorisatie kan geregeld worden wie, wat met welke gegevens kan doen. Autorisatie *op groep* houdt in dat je toegang krijgt tot bepaalde gegevens omdat je tot een bepaalde groep behoort, je mag in principe alles met die gegevens doen (bv toegang tot delen van de P: schijf). Autorisatie *op rol* houdt in dat je toegang krijgt tot gegevens omdat jij binnen de organisatie een bepaalde rol vervult (inkoper, lokaalplanner,..). Een autorisatie *op mutatie* is nog sterker omdat daarbij niet alleen de toegang tot het gegeven wordt geregeld maar ook wat je met dat gegeven mag doen (lezen, opvoeren, wijzigen, verwijderen,..). In praktijk zie je vaak combinaties van rollen met mutaties (ERP is hier een voorbeeld van).

Authenticatie: Gaat om het verifiëren van iemands identiteit en dus hebben de eisen hier betrekking op hoe iemand kan aantonen dat hij is wie hij zegt te zijn. Authenticatie kan plaats vinden op basis van iets dat men *weet (b.v. wachtwoord)*, *heeft (b.v. token)*, of *is (biometrische kenmerken b.v. vingerafdruk)*. Er is sprake van twee-factor authenticatie (of sterke authenticatie) als iemand zich moet authenticeren aan de hand van een combinatie van twee van deze drie.

De minimale eis is hier een persoonsgebonden gebruikersnaam en wachtwoord. Dit maakt het mogelijk om acties te traceren naar individuele gebruikers. Gegeven de wachtwoorddiscipline van de gemiddelde UT- gebruiker is gebruikersnaam/wachtwoord een relatief zwakke vorm van authenticatie. Bij een classificatie “gevoelig of kritiek” wordt dit intern voldoende geacht (men heeft immers ook nog de toegang tot een personeelswerkplek nodig). Heeft men echter mutatierecht en wil men van buitenaf toegang dan dient hier twee-factor authenticatie van toepassing te zijn. Heeft men van buitenaf alleen kijkrechten dan is twee-factor authenticatie vanuit het oogpunt van integriteit niet van belang, men kan namelijk niets aan deze gegevens wijzigen. Het is te overwegen om voor bedrijfsmiddelen met de classificatie “kritiek” ook intern twee-factor authenticatie toe te passen.

Audittrail: Hiermee kunnen specifieke mutaties terug gevoerd worden op individuele gebruikers. Biedt mogelijkheden om onopzettelijke fouten en frauduleuze handelingen te traceren naar een gebruiker.

Inputvalidatie: Hiermee kan je in een vroeg stadium tot op zekere hoogte foutieve invoer voorkomen (denk bijvoorbeeld aan een cijfer dat tussen 0 en 10 moet liggen waar dan ook geen 11 ingevoerd moet kunnen worden). Dat deze validatie aan de serverkant gebeurt en niet aan de cliënt kant (op de pc) is met name bij webapplicaties een belangrijk issue. Onvoldoende ingerichte inputvalidatie maakt een webapplicatie kwetsbaar voor “Cross site scripting”. Dit is een aanvalstechniek waarbij een hacker via de “inputschermen” van een webapplicatie kleine programmaatjes naar de server stuurt en die daar laat uitvoeren.

Functiescheiding: Dit is een organisatorische maatregel die overwogen moet worden voor bepaalde processen. De fraudegevoeligheid van processen kan verkleind worden door er voor te zorgen dat er meer dan één persoon nodig is om de fraude te kunnen plegen. (Denk aan het inkoopproces, in dit proces is het onverstandig het plaatsen van een bestelling, de goederenontvangst en het betaalbaar stellen van de factuur door dezelfde persoon te laten uitvoeren.)

Servercertificaten / SSL: Door het gebruik van servercertificaten kunnen gebruikers weten of de website die ze benaderen ook de juiste website is en niet een website die door een hacker is nagebouwd. Daarnaast wordt informatie die de gebruiker met zo’n server uitwisselt versleuteld

(geëncrypt) over de lijn verzonden. Servercertificaten kunnen ook gebruikt worden in de communicatie tussen servers onderling.

Training van gebruikers: Is een organisatorische maatregel. Integriteit van bedrijfsmiddelen is gebaat bij een juist gebruik ervan. Gebruikers dienen daarbij ook bewust gemaakt te worden van de beveiligingsissue die spelen rondom de processen waar zij onderdeel van zijn.

Versiebeheer documenten incl. timestamping: Ter voorkoming dat documenten hetzelfde lijken te zijn terwijl ze dat niet zijn.

Periodieke controle proces/data: Als integriteit kritiek is zal regelmatig bezien moeten worden of proces en data nog aan de integriteitseisen voldoen en ook volgens afspraken worden uitgevoerd.

Gebruik van digitale handtekening in communicatie: Als de ontvangende partij er zeker van moet kunnen zijn dat een bericht afkomstig is van de verzendende partij dan moet hij dit via de digitale handtekening kunnen verifiëren (b.v. bij mail kan dit van belang zijn). Een digitale handtekening werkt twee kanten uit, enerzijds weet de ontvanger met zekerheid wie de mail verstuurd heeft anderzijds kan de verzender niet ontkennen dat betreffende mail door hem verstuurd is (non repudiation principle). Juridisch heeft een digitale handtekening dezelfde status als een gewone handtekening. Deze zijn dus ook geldig voor ondertekening van contracten e.d.

II.3 Toelichting op maatregelen vertrouwelijkheid

Een aantal maatregelen met als uitgangspunt bescherming van de integriteit zijn ook van toepassing in relatie tot vertrouwelijkheid. Dit betreft met name maatregelen die te maken hebben met authenticatie en autorisatie. Maatregelen op dat gebied zorgen ervoor dat alleen daartoe gerechtigde personen wijzigingen kunnen doorvoeren (integriteit) en bepaalde informatie kunnen zien (vertrouwelijkheid). Deze maatregelen komen in de matrix dan ook in beide kolommen voor.

Authenticatie: zie hierboven.

Autorisatie: zie hierboven.

Sterk wachtwoordbeleid: Overeenkomstig de huidige praktijk.

Publieke netwerken: Vertrouwelijke informatie mag niet via het publieke netwerk (internet) benaderbaar zijn. Dat betekent dat deze informatie dan ook niet logisch in de DMZ geplaatst mag worden. In de DMZ (demilitarized zone) staan services die vanaf het internet benaderbaar moeten zijn zoals een portaal. Moet deze informatie toch vanuit huis toegankelijk zijn dan moet gedacht worden aan VPN (virtual private network) voorzieningen.

Encryptie datatransport: Versleuteling van datatransport wordt toegepast om afluisteren te voorkomen. Er zijn verschillende tools in omloop om dataverkeer af te luisteren. Dit zijn overigens niet alleen maar tools die door hackers gebruikt worden maar ook door netwerkbeheerders om problemen op te sporen.

Encryptie van opslag: Veel informatie wordt tegenwoordig meegenomen op mobiele devices (notebooks, PDA, USB memorysticks, mobiele telefoon,..). Mobiele devices zijn echter diefstal gevoelige items daarnaast kunnen USB memorysticks makkelijk vergeten worden. Vertrouwelijke data opgeslagen op deze devices dient dan ook beschermt te worden tegen lezen door ongeautoriseerde personen.

Gecontroleerde afvoer: Zowel digitale media waarop gevoelige informatie is opgeslagen als de papieren versie daarvan dienen op een gecontroleerde manier afgevoerd te worden. De beste manier is om harde schijven te vernietigen en niet her te gebruiken. Wissen alleen is niet voldoende (in de literatuur wordt gesteld dat pas na zeven keer overschrijven een harde schijf geen terug te halen informatie meer bevat.) Geprinte versie van vertrouwelijke informatie behoren door de papierversnipperaar gehaald te worden.

Clear desk policy: Vertrouwelijke informatie hoort ook na werktijd niet rond te slingeren op bureaus. Kamers zijn immers voor veel personen toegankelijk (schoonmakers, technisch personeel, servicedeskmedewerkers, collega's, BHV'ers.)

Voldoen aan WBP: De Wet Bescherming Persoonsgegevens legt een aantal verplichtingen op met betrekking tot de zorgvuldige wijze waarop met persoonsgegevens moet worden omgegaan. Het vrijstellingsbesluit gekoppeld aan deze wet ontslaat de Universiteit voor bepaalde gegevensverwerkingen van de verplichting tot melding bij het CBP. Dit neemt niet weg dat de Universiteit ook voor deze verwerkingen wel aan de wet moet voldoen en dus moet beschikken over een *doelomschrijving, een grondslag voor verwerking met indien van toepassing een privacytoets en instemming van de URaad.* Deze dienen vastgelegd te zijn en indien de verwerking niet onder het vrijstellingsbesluit valt dan dient ook melding bij het CBP gemaakt te worden (tenzij de Universiteit Twente over een functionaris gegevensbescherming zou beschikken, deze dient aangemeld te zijn bij het CBP en neemt de controle verantwoordelijkheid van het CBP over).

Distributie van gegevens: De eigenaar van vertrouwelijke gegevens dient toestemming te geven voor distributie van deze gegevens. Dit geldt zowel voor het gebruik in bijvoorbeeld rapportages als het gebruik van gegevens door andere systemen.

Printen: Als informatie al uitgeprint moet worden dan dient dit in een veilige printomgeving te gebeuren. Omdat geprinte informatie per definitie niet versleuteld is dient de houder voor het gebruik van kritieke gegevens uitdrukkelijk toestemming te verlenen voor het gebruik ervan buiten de gebouwen van de Universiteit Twente.

Testomgeving: Omdat voor testdoeleinden vaak een kopie van de productiedatabase gebruikt wordt is het van belang om voor vertrouwelijke informatie ook in de testomgeving eenzelfde vertrouwelijkheidregime als in de productieomgeving te handhaven. Voor kritieke vertrouwelijke gegevens mag geen kopie van de productiedatabase gebruikt worden ten behoeve van testdoeleinden. Of een gegeven kritiek is, is soms ook in de tijd bepaald. Documenten m.b.t. fusiebesprekingen kunnen tijdens de besprekingen kritiek vertrouwelijk zijn maar nadat de fusie een feit is geworden wellicht niet meer.