UNIVERSITEIT
GENT

INFORMATIEBEVEILIGING

TECHNISCHE EN ORGANISATORISCHE MAATREGELEN AAN DE UGENT

Niet vertrouwelijk, versie dd. 17 februari 2022.

Inhoud

1 Inleiding

Dit document geeft een overzicht van een aantal strategieën en maatregelen die binnen de Universiteit Gent (UGent) worden gevolgd teneinde de beveiliging van data en informatie optimaal te garanderen. Het vernoemt maatregelen die genomen worden om de integriteit, de beschikbaarheid, de vertrouwelijkheid en de cyberweerbaarheid, en tevens de niet-weerlegbaarheid, de authenticiteit van informatie en de auditeerbaarheid van informatie verwerkende systemen te garanderen. Dit overzicht is niet exhaustief, niet alle genomen maatregelen worden vermeld.

2 Algemeen beveiligingsbeleid en organisatie van informatiebeveiliging

2.1 Informatieveiligheidsbeleid

De UGent beschikt over een modulair gegevensbeschermings- en informatieveiligheidsbeleid. De verschillende modules van dit beleid werden geleidelijk opgebouwd in de voorbije jaren, het geheel van het beleid wordt jaarlijks geëvalueerd en waar nodig geüpdatet.

Het beleid is aangepast aan de context van de UGent, het is conform de bepalingen van de toepasselijke wetgeving en relevante besluiten, en van de Algemene Verordening Gegevensbescherming.

Het informatieveiligheidsbeleid van de UGent omvat onder andere:
- procedures voor de bescherming van de informatiegegevens in elektronische berichten;
- procedures voor de bescherming tegen het verlies van gegevens;
- procedures voor de bescherming tegen malware (bijgewerkte antivirus, firewall,...);
- een beleid inzake het beheer van de toegang van de gebruikers waarbij de toegang tot de systemen en diensten voorbehouden wordt voor de gemachtigde gebruikers en een niet-gemachtigde toegang voorkomen wordt;
- een geschikt beleid met betrekking tot wachtwoorden;
- procedures voor de bescherming van de toegang tot de servers;
- procedures voor de bescherming van de toegang tot het netwerk;
- procedures voor de bescherming van de werkposten;
- procedures met betrekking tot de classificatie van de informatiegegevens volgens hun waarde of hun kritieke of gevoelige aard in geval van wijziging of niet-toegestane verspreiding en met betrekking tot de gevolgen van de classificatie.

De informatica-infrastructuur voor de digitale bewaring van zeer vertrouwelijke gegevens is beschermd tegen elk bekend risico van individuele indringing en tegen ongeoorloofde toegang tot de informatie die ze bevat. Daartoe is ze beveiligd op een wijze zodat iedere vorm van individuele indringing of ongeoorloofde toegang tot de bestanden wordt gedetecteerd. In geval van een dergelijke detectie, worden onmiddellijk de nodige tegenmaatregelen, waaronder alarmeringen, genomen. Dit beveiligingssysteem functioneert autonoom ten aanzien van de informaticasystemen gebruikt voor de digitale bewaring van deze zeer vertrouwelijke gegevens.

2.2 Verantwoordelijke voor IT-beveiliging

De UGent heeft een IT-Security Officer aangewezen die verantwoordelijk is voor de IT-security en tevens voor de informatie- en databeveiliging. De IT-Security Officer is permanent uitgenodigd expert in de ICT-Commissie van de UGent en is lid van de Commissie Privacy en Gegevensbescherming. De IT-Security Officer rapporteert aan de directeur van de Directie ICT.

2.3 Verantwoordelijke voor controle op gegevensbescherming

De UGent heeft een Data Protection Officer aangewezen die verantwoordelijk is voor het interne toezicht op de naleving van de AVG en de nationale regelgeving inzake gegevensbescherming. De Data Protection Officer werkt hiervoor samen met de IT-Security Officer, en wordt bijgestaan door een Commissie Privacy en Gegevensbescherming met vertegenwoordigers uit alle geledingen van de UGent. De Data Protection Officer rapporteert aan de directeur van de Directie Bestuurszaken en aan de rector.

2.4 Verantwoordelijkheden op vlak van informatiebeveiliging en gegevensbescherming

Verantwoordelijkheden van de medewerkers van de UGent zijn formeel gedocumenteerd en gepubliceerd in het modulair gegevensbeschermings- en informatieveiligheidsbeleid.
Belangrijke documenten daar zijn de “Generieke gedragscode voor de verwerking van persoonsgegevens en vertrouwelijke informatie” en het “Reglement voor correct gebruik van de ICT-infrastructuur van de UGent” (d.i. de Acceptable Use Policy).

2.5 Risicoanalyse, beheer en controle

De UGent voert periodiek risicoanalyses uit van de genomen beveiligingsmaatregelen en doet controles voor wat betreft de naleving van de verschillende informatiebeveiligingsprocedures.

Voor wat betreft centrale IT-dienstverlening is de verantwoordelijkheid daarover belegd bij de IT-Security Officer, die daarvoor samenwerkt met de Directie ICT en met de Data Protection Officer.

Voor algemene risicobeheersing op gebied van gegevensbescherming en van IT-security organiseert de dienst Interne Audit van de UGent selectief audits. Resultaten van dergelijke audits worden gecommuniceerd aan het auditcomité van de UGent en aan de Raad Van Bestuur van de UGent.

Voor wat betreft decentrale IT-toepassingen wordt de verantwoordelijkheid voor de risicobeheersing gedeeld met decentrale IT-beheerders. Het modulair informatieveiligheidsbeleid van de UGent voorziet in richtlijnen voor IT-beheerders en voor IT-eindgebruikers voor risicobeheersing op gebied van informatiebeveiliging.

3 Veilig personeelsbeleid

3.1 Training over belang van beveiliging en omgang met persoonsgegevens

De UGent communiceert op regelmatige basis over het belang van informatiebeveiliging naar alle medewerkers en studenten. Online trainingsmodules worden ter beschikking gesteld van de medewerkers. Waar nodig worden specifieke trainings- en/of informatiesessies georganiseerd, bijvoorbeeld voor startende medewerkers.

Alle systeemingenieurs van de Directie ICT van UGent volgen een doorgedreven opleiding bij indiensttreding. Op regelmatige tijdstippen worden er bijkomende opleidingen voorzien om te kunnen garanderen dat de kennis van de betrokken werknemers accuraat en up-to-date blijft.

3.2 Autorisaties

De UGent implementeert en handhaaft authenticatie- en autorisatiebeheersystemen die de toegang controleren tot systemen die persoonsgegevens bevatten. Waar mogelijk wordt gewerkt met rol-gebaseerde autorisaties.

Minimaal is de logische toegang tot elk informatiesysteem beveiligd met strikt persoonlijke credentials (gebruikersnaam/wachtwoord). Authenticatie en autorisaties zijn steeds gebaseerd op de informatie die aanwezig is in redundant uitgebouwde centrale repositories (LDAP en AD, deels on-prem, deels in cloud met AAD in een hybride setup).

Toekenning van accounts en autorisatie gebeurt uitsluitend op basis van door het bestuur bekrachtigde regels, en is rechtstreeks gekoppeld met de primaire bronnen voor personeels- en studentenbeheer, en vervalt dan ook automatisch wanneer het statuut van de betrokkene vervalt. De regels voor correct gebruik van de persoonlijke credentials en account zijn beschreven in de Acceptable Use Policy van UGent.

3.3 Functiescheiding (segregation of duties)

De UGent past zo goed als mogelijk functiescheiding toe om te vermijden dat personen toegang krijgen tot gegevens waarvoor ze geen toegang nodig hebben voor de uitoefening van hun taak. Waar mogelijk wordt dit technisch afgedwongen.

4 Fysieke beveiliging van werk- en kantoorruimtes

De UGent beperkt de toegang tot werk- en kantoorruimtes waar persoonsgegevens of vertrouwelijke informatie verwerkt worden in kader van haar opdracht. Waar nodig en op basis van risicoanalyse wordt toegang strikt beperkt tot geïdentificeerde en geautoriseerde personen. Waar nodig worden inbraakbeveiliging en/of badge-lezers geïnstalleerd, dit alles om ongeoorloofde toegang te vermijden.

De verantwoordelijkheid voor het beheersen van de beveiliging van de fysieke toegang tot de gebouwen van de UGent ligt bij de Coördinator Security van het PermanentieCentrum van de UGent.

5 Beveiliging van datacenters

5.1 Inleiding

De data die zich binnen de verschillende centrale server- en opslagsystemen van de UGent bevindt, maakt deel uit van informatiesystemen in twee gescheiden datacenters binnen Gent. Het primaire datacenter bevindt zich op Campus Sterre, het secundaire datacenter is ondergebracht op Campus Ardoyen.

5.2 Fysieke beveiliging van datacenters

Fysieke toegang tot de eigen datacenters wordt strikt beheerd en gecontroleerd en is beveiligd conform industrienormen, o.a. met videobewaking en inbraakalarm.

Toegang tot de datazalen is beveiligd met badgelezers. De serverzalen in elk datacenter zijn enkel toegankelijk voor de daartoe geautoriseerde systeemingenieurs van de UGent. In geval externen fysiek toegang nodig hebben tot één van de datacenters, gebeurt dit steeds onder begeleiding en toezicht van een systeemingenieur van de Directie ICT van UGent. De uitreiking van badges gebeurt conform een strikt fysiek identificatieproces waarbij elke werknemer zich persoonlijk moet aanmelden voor het verkrijgen van zijn badge. Alle toegangen kunnen centraal worden uitgelezen zodat op elk moment kan worden nagegaan wie in welke ruimte is binnen geweest.

In elk datacenter zijn de nodige professionele voorzieningen getroffen om een eventuele brand snel te blussen, met minimale impact op de IT-systemen. De temperatuur en vochtigheid binnen de ruimtes wordt permanent gemeten en genereert alarmen indien bepaalde drempelwaarden worden overschreden.

Voor toepassingen en data die gehost worden in externe cloudsystemen wordt vooraf een analyse gemaakt of bijhorende risico’s voldoende onder controle en aanvaardbaar zijn.

5.3 Redundantie

Alle faciliteiten en services in de eigen datacenters zijn met voldoende redundantie beveiligd tegen onvoorziene uitvallen.

Elk datacenter is uitgerust met professionele installaties om de continuïteit van enerzijds stroomvoorziening (d.m.v. UPS-installaties en diesel-generatoren) en koeling (door middel van ontdubbelde koelmachines en ventilo's) te garanderen.

De UGent beschikt naast het primaire datacenter over een fail-over datacenter. De meest kritische informatiesystemen zijn redundant uitgebouwd over de twee datacenters heen, zodat bij uitval van één enkel systeem of zelfs het verlies van een volledig datacenter nog steeds de operationele werking van verschillende noodzakelijke diensten binnen UGent verzorgd kan worden.

5.4 Noodherstel (Disaster Recovery Planning)

De UGent beschikt over noodherstelplannen om in geval van calamiteiten met de IT-infrastructuur in de centrale datacenters de downtime tot een minimum te beperken. De noodherstelplannen worden op regelmatige basis bijgewerkt en de noodscenario's worden jaarlijks getest en geëvalueerd.

Een dubbele back-up- en restorestrategie, enerzijds op basis van snapshot-technologie en datareplicatie en anderzijds door middel van dagelijkse back-upkopieën, garandeert dat het verlies van data in geval van een calamiteit in één van de centers tot een minimum beperkt wordt. Back-ups worden genomen op specifieke back-upopslagsystemen. Een identieke kopie van alle back-up data wordt in beide datacenters bewaard.

6 Beveiliging van het intern netwerk

Het interne netwerk van de UGent (UGentNet) is sterk gecompartimenteerd en uitgerust met geavanceerde controlemechanismen (firewall, intrusion detection & prevention) die het interne netwerk op gepaste wijze beschermen tegen ongeoorloofde toegang en ongewenste acties van buitenaf. Hiervoor wordt ook samengewerkt met Belnet, de Internet Service Provider voor de UGent.

Voor de draadloze netwerken worden up-to-date encryptieprotocollen gehanteerd om de getransfereerde data maximaal te beschermen.

7 Beveiliging van data at rest

7.1 Versleuteling van gegevens

De UGent voert het beleid dat digitale persoonsgegevens en vertrouwelijke informatie op centraal aangeboden en ondersteunde opslagmogelijkheden moeten worden bewaard. Externe clouddiensten mogen niet voor het opslaan van data met hoog risico gebruikt worden, tenzij de data vooraf (d.i. client-side) op een veilige en betrouwbare manier versleuteld worden met cryptografische tools.

7.2 Antivirus en beveiligingsupdates

Vaste en mobiele gebruikersapparatuur wordt beveiligd door up-to-date antimalware tools. De UGent voorziet de centrale IT-systemen en gebruikersapparatuur onder centraal beheer van de laatste beveiligingsupdates. Deze worden zo goed mogelijk opgevolgd en geïnstalleerd volgens een betrouwbaar patchmanagementproces.

7.3 Kwaadaardige Software

De UGent voert anti-malwarecontroles uit om te voorkomen dat kwaadaardige software schade aanricht, bv. ongeautoriseerde toegang krijgt of de toegang tot eigen data onmogelijk maakt (beveiliging tegen gijzelsoftware).

7.4 Logging van toegangen

De ICT-infrastructuur van de UGent wordt door ICT-systeembeheerders gecontroleerd met logging en monitoring, om de goede werking ervan te kunnen verzekeren en om misbruik op te sporen en te voorkomen. Het niveau van detail is niet meer en de bewaarduur niet langer dan nodig om dit doel te bereiken.

Afhankelijk van het type data of informatie en de graad van confidentialiteit ervan, is de logging minder of meer gedetailleerd. Voor kritische informatiesystemen worden toegangen en acties uitgebreid gelogd. Gegevens uit deze logging zijn vertrouwelijk en worden enkel vrijgegeven na een door het bestuur aanvaarde formele vraag (bvb. een gerechtelijk bevelschrift).

8 Beveiliging van data in motion

De UGent maakt gebruikt van up-to-date encryptieprotocollen (TLS, HTTPS, VPN) voor transmissie van data binnen en buiten het UGent netwerk.

9 Beveiliging van UGent accounts

UGent accounts worden beveiligd door een wachtwoord dat minstens jaarlijks moet vernieuwd worden. De wachtwoorden moeten een zeker niveau van complexiteit hebben. Deze vereisten worden ook technisch afgedwongen. Alle UGent accounts zijn bijkomend beveiligd met multifactor authenticatie.

10 Beveiliging van IT-systemen & servers

De UGent past risicobeheersing toe voor de beveiliging van al haar IT-systemen. Kritische systemen en kritische toepassingen worden op regelmatige basis aan een veiligheidstest door een onafhankelijke derde onderworpen. De vereisten voor de bescherming van gegevens en systemen worden waar nodig ook geanalyseerd en gespecificeerd in samenwerking met IT-leveranciers.

11 Incidentmanagement

Alle centraal beheerde informatiesystemen worden permanent gemonitord. De Directie ICT heeft een permanentieregeling 24/24 en 7/7 actief om in geval van een storing onmiddellijk te kunnen ingrijpen.

Voor de triage en afhandeling van incidenten heeft de Directie ICT een draaiboek uitgewerkt voor alle IT-incidenten, inclusief die met persoonsgegevens.
Wanneer de UGent optreedt als verwerker van persoonsgegegens en in geval van een gegevensbeveiligingsincident dat een belangrijke impact heeft op de vertrouwelijkheid of integriteit

van die persoonsgegevens, informeert de UGent de verwerkingsverantwoordelijke (en eventueel andere belanghebbenden) zonder onredelijke vertraging.

Het beheer van incidenten wordt geregistreerd en opgevolgd via een centraal beheersysteem. Maandelijks wordt een rapportering opgemaakt over alle incidenten die zich hebben voorgedaan, over hun impact, over de oplossing en over de ‘lessons learned’.

Om de kans op incidenten tot een minimum te reduceren, worden onderhoudsvensters ingepland op vaste tijdstippen om de nodige proactieve onderhoudsactiviteiten op de systemen te kunnen uitvoeren. In geval van dringende onderhoudswerkzaamheden, worden urgentie-onderhoudsvensters ingelast. Tijdens een onderhoudsvenster kunnen (een groep van) systemen tijdelijk onbeschikbaar zijn. Elk onderhoudsvenster wordt daarom d.m.v. een brede communicatie van de eventuele impact ervan aangekondigd doorheen de organisatie (via intranet).

12 Bijkomende maatregelen

Bovenstaande elementen beschrijven het algemene, centraal gecoördineerde beveiligingsbeleid van de centrale IT-dienstverlening aan de UGent.
Op basis van meer gedetailleerde risicoanalyse worden bijkomend passende maatregelen genomen voor specifieke verwerkingen op centrale of decentrale IT-infrastructuur, in het bijzonder in het kader van onderzoeksprojecten die met persoonsgegevens of vertrouwelijke informatie werken.