Landstede Groep

Informatiebeveiligings-en privacy beleid

Beleidsplan

Versie: Definitief, april 2022

Inhoud

1. Documentversie

Datum	Versie	Aanpassing	Afgestemd met
4-6-2020	1.1	Als basis het vastgesteld beleid gebruikt. Vanuit de Peer review het volgende toegevoegd in bijlage B: • Wachtwoord beleid • Beleid beveiligde inlogprocedures • Toegang tot netwerk en netwerkdiensten. • Clear Screen beleid • Clear Desk beleid	• M. van Gelder (functionaris gegevens bescherming) • B.Lammers (informatiemanagement) • E.Brongers (Adviseur ICT, & CERT-SERT)
14-4-2021	1.2	Het CvB heeft besloten dat de IBP-Coördinator bij Dienst Organisatie Ondersteuning wordt ondergebracht. Verder is een extra rol bij Concern Control ondergebracht: De Interne Auditor.	CvB
14-4-2022	2.0	Beleid is definitief vastgesteld	CvB

2. Inleiding

Landstede Groep biedt onderwijs voor jong en oud, en wil actief een brug slaan tussen onderwijs, de omgeving en de samenleving, met waarde(n)vol leren, leven en werken. Bij het uitvoeren van deze missie is het noodzakelijk zorgvuldig om te gaan met de gegevens die we van de leerling, de student en de medewerker verwerken.

Een veilige opslag van informatie is van essentieel belang voor de continuïteit van de bedrijfsvoering van de organisatie. Zowel op papier als geautomatiseerd zijn wij bij ons dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. Onze organisatie en onze informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), et cetera. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren.

2.1. Informatiebeveiliging en privacy

Informatiebeveiliging (IB) is een geheel aan maatregelen om te beschermen tegen de risico's en bedreigingen met betrekking tot informatie en ICT-infrastructuur. Het richt zich op drie aspecten:

- **Beschikbaarheid:**
  De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.
- **Integriteit:**
  De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de ICT-dienstverlening waarborgen.
- **Vertrouwelijkheid:**
  De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

Privacy (P) gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving (AVG[1]).
Door privacy (P) te koppelen aan informatiebeveiliging (IB), wordt privacy een integraal onderdeel van het Informatiebeveiliging en privacy beleid (IBP beleid).

[1] *AVG = Algemene Verordening Gegevensbescherming*

3. Doel en reikwijdte

Het informatiebeveiligings- en privacy (IBP) beleid heeft betrekking op het verwerken van de gegevens van alle betrokkenen binnen de Landstede Groep waaronder in ieder geval alle medewerkers, studenten, leerlingen, gasten, bezoekers en externe relaties.

Het beleid is bedoeld als kader om de kwaliteit van de verwerking en de beveiliging van persoons-gegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.
Uitgangspunt is dat persoonlijke levenssfeer van de betrokkene wordt gerespecteerd. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn.

Het informatiebeveiligings- en privacy beleid heeft raakvlakken met andere beleidsgebieden, te weten:

- Algemene veiligheids- en beveiligingsbeleid: met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang- en beveiliging, crisismanagement, huisvesting en ongevallen.
- ICT-beleid: met als aandachtsgebieden een goede ICT-infrastructuur die het veilig opslaan, verwerken en uitwisselen van gegevens mogelijk maakt.
- Personeels- en organisatiebeleid: met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties.
- Beleid ten aanzien van risicomanagement: met als aandachtsgebieden Interne controle / audit, Financieel en business control en Security en privacy.
- Informatiebeleid (BIP/LARA)

4. Uitgangspunten

De belangrijkste beleidsuitgangspunten binnen de Landstede Groep zijn voor wat betreft Informatiebeveiliging en Privacy (IBP):

1. Informatiebeveiliging en privacy dient te voldoen aan alle relevante wet- en regelgeving

2. De volgende stichtingen zijn als rechtspersonen eigenaar van de informatie die onder haar verantwoordelijkheid wordt verzameld en geproduceerd:
   - Stichting Agnieten College / De Boog
     - BRIN-nummer = 02VT en 05VN
     - Bestuursnummer = 41430
   - Stichting Ichthus College
     - BRIN-nummer = 02VB en 07ZI
     - Bestuursnummer = 41429
   - Stichting Vechtdal College
     - BRIN-nummer = 02UX
     - Bestuursnummer = 40722
   - Stichting Chr. VMBO Harderwijk e.o.
     - BRIN-nummer = 02EX
     - Bestuursnummer = 41158
   - Stichting Landstede
     - BRIN-nummer = 01AA
     - Bestuursnummer = 40810

   Landstede Groep en daarmee ook de genoemde stichtingen respecteert de rechten van de werknemers die informatie produceren: Mail die wordt geproduceerd is niet zonder meer in te zien of te gebruiken door de werkgever. Hiervoor moet de werkgever legitieme redenen hebben, zoals beveiligingsrisico's of het vermoeden van een juridische overtreding.

3. De Landstede Groep maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy

4. Informatiebeveiliging en privacy is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassingen gewenst zijn

5. Veilig en betrouwbaar omgaan met informatie is een verantwoordelijkheid van iedereen

6. Er wordt van alle medewerkers, studenten, leerlingen, gasten, bezoekers en externe relaties verwacht dat zij zich "fatsoenlijk" gedragen met een eigen verantwoordelijkheid

7. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen

8. Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid

4.1. Informatiebeveiliging

Binnen de Landstede Referentie Architectuur (LaRa) zijn de volgende principes opgenomen in het kader van informatiebeveiliging:

1. Business architectuur
   - Veiligheid en privacy is geborgd
2. Informatie architectuur
   - Informatievoorziening is gepersonaliseerd
   - Informatie wordt beheerd en bewaakt
   - Informatie is veilig
   - Informatie is een activa, kapitaalgoed
3. Applicatie architectuur
   - Applicaties worden beheerd en bewaakt
   - Applicaties zijn veilig
4. Technische (infra) architectuur
   - Beveiliging is een integraal onderdeel van de gehele technische infrastructuur

4.2. Privacy

De Landstede Groep hanteert de vijf vuistregels voor privacy:

1. **Doelbepaling en doelbinding:** persoonsgegevens worden allen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarop ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken, ze staan in verhouding tot het doel. Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** de school legt aan betrokkenen op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde informatiebeveiliging en privacy beleid en vindt ongevraagd plaats. Daarnaast hebben de betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun persoonsgegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

5. Wet- en regelgeving

Binnen de Landstede Groep wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

5.1. Wet Educatie en Beroepsonderwijs (WEB)

De Landstede Groep heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studenten administratie en met de studieresultaten is gewaarborgd.

5.2. Wet op het primair onderwijs en/of Wet voortgezet onderwijs

Landstede Groep is er voor alle leerlingen, ook degenen die extra ondersteuning nodig hebben. Waar mogelijk zorgt Landstede Groep voor een passende onderwijsplek. De registratie wordt bijgehouden in een registratie en volgsysteem waarbij alleen de meest betrokken personen beschikken over de privacygevoelige gegevens.

5.3. Wet goed onderwijs en goed bestuur PO/VO

De wet kent twee pijlers: goed onderwijs én goed bestuur.

Goed onderwijs: minimumeisen voor kwaliteit
Goed onderwijs betekent dat iedere school verantwoordelijk is voor het geven van kwalitatief goed onderwijs. Dit begint er mee dat iedere school moet voldoen aan een wettelijke vastgesteld niveau van basiskwaliteit.

Goed bestuur: functiescheiding intern toezicht – bestuur
Goed bestuur betekent dat ieder bestuur wordt geacht te functioneren volgens algemene principes van goed bestuur. Als onderdeel daarvan stelt de wet als voorwaarde dat iedere rechtspersoon die met publieke gelden scholen in stand houdt, het interne toezicht op het bestuur goed regelt (functiescheiding tussen intern toezicht en het bestuur).
De Landstede Groep heeft voor een organisatievorm gekozen, die bestaat uit een College van Bestuur (CvB), directies (per eenheid/stichting) en een medezeggenschap voor het interne toezicht. De Raad van Toezicht verzorgt het externe toezicht.

5.4. Algemene Verordening Gegevensbescherming (AVG)

De Landstede Groep heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiligings- en privacy beleid.

De ingangsdatum van de AVG is 25 mei 2016 en de inwerkingtreding is 25 mei 2018. De AVG komt in plaats van de Wbp (Wet bescherming persoonsgegevens).

5.5. Leerplichtwet

Voor leerlingen van 5 tot 16 jaar heet dit de leerplicht. Voor jongeren tussen 16 en 18 jaar heet dit de kwalificatieplicht.

De Landstede Groep neemt de benodigde maatregelen om schooluitval van jongeren tegen te gaan. Indien dit toch het geval is, werkt de Landstede Groep zo goed mogelijk mee om de kansen van startende jongeren op de arbeidsmarkt te vergroten.

5.6. Archiefwet

De Landstede Groep houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

5.7. Auteurswet

De Landstede Groep verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat De Landstede Groep het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

5.7.1. Portretrecht

Voor alle portretten gemaakt voor marketingdoeleinden zijn met de geportretteerde afspraken gemaakt, die vastgelegd worden in een overeenkomst.
Tevens is in de folder Integriteit in de praktijk vastgelegd hoe er binnen Landstede Groep met het delen van foto's en opnames wordt omgegaan.

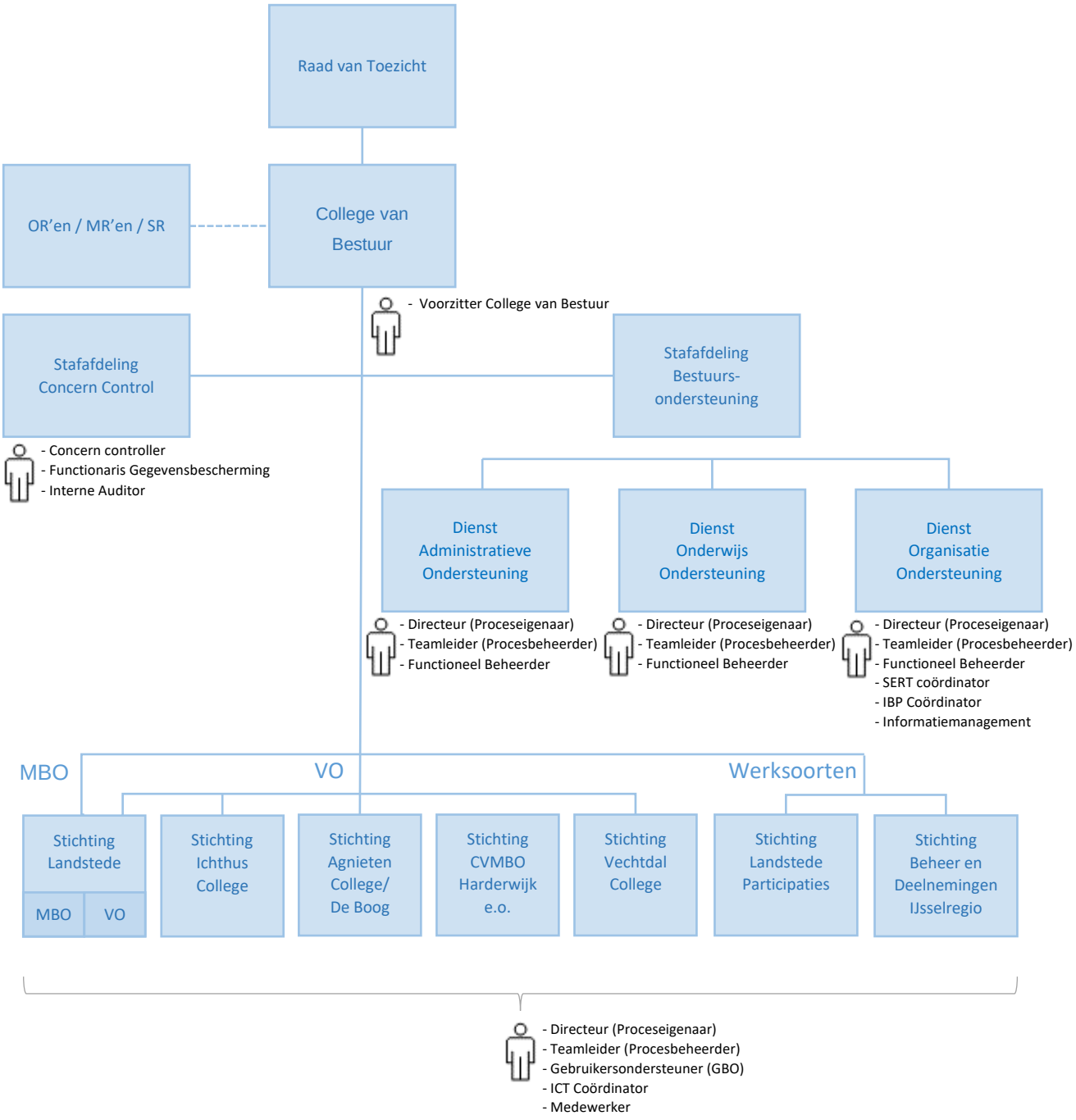
5.8. Wetboek van Strafrecht

In het Wetboek van Strafrecht zijn de laatste decennia een aantal specifieke bepalingen opgenomen over de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat "enige beveiliging" vereist is alvorens er sprake *kan zijn* van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling.

Naleving van dit informatiebeveiligingsbeleid en implementatie van de basismaatregelen bij de Landstede Groep moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van het Wetboek van Strafrecht.

6. Organisatie, taken en verantwoordelijkheden

Het doel van de informatiebeveiligings- en privacy organisatie is het monitoren en verbeteren van het informatiebeveiligings- en privacy beleid binnen de organisatie.



Figuur 1: Verantwoordelijke IBP functionarissen binnen het organisatie organogram

Voorzitter College van Bestuur
Het College van Bestuur (CvB) is eindverantwoordelijk voor de informatiebeveiligings- en privacy beleid. Tevens is ze verantwoordelijk voor het opstellen en uitdragen van het algemene organisatiebeleid en de rol van informatiebeveiligings- en privacy beleid daarbinnen. Daarnaast houdt het College van Bestuur controle op de naleving en evaluatie van het afgesproken beveiligingsniveau. Het vernieuwde informatiebeveiligings- en privacy beleid wordt jaarlijks opnieuw door het College van Bestuur vastgesteld.

Concern controller
Vanuit Concern Control wordt een Functionaris Gegevensbescherming en Interne Auditeur aangesteld en hiermee is de Concern Controller de directe leidinggevende van deze twee functionarissen.
De Concern Controller is eindverantwoordelijk voor de jaarlijkse planning en control cyclus, waarmee onder andere de inhoud en effectiviteit van het informatiebeveiligings- privacy beleid wordt getoetst.

Functionaris Gegevensbescherming
De functionaris gegevensbescherming (FG) evalueert en ontwikkelt het privacy (P) beleid. Het privacy beleid is een integraal onderdeel van het informatiebeveiligings- en privacy (IBP) beleid, wat in een co creatie met informatiemanagement wordt opgesteld. Gezamenlijk borgen ze dat deze jaarlijks wordt vastgesteld door het College van Bestuur.
De functionaris gegevensbescherming draagt zorg voor de implementatie en uitvoering van het informatiebeveiligings- en privacy (IBP) beleid, met name de privacy componenten. Bewaakt het IBP-beleid en doet verbetervoorstellen, indien niet aan het beleid wordt voldaan. Tevens zorgt de functionaris gegevensbescherming voor de afhandeling van informatiebeveiligingsincidenten.

Om de bewustwording te vergroten wordt er door de functionaris gegevensbescherming jaarlijks een bewustwordingscampagne ontwikkeld en over de organisatie uitgerold.

IBP-Coördinator
De IBP-coördinator heeft een sturende rol. Geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag. De IBP-coördinator moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen de Landstede Groep
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De afhandeling van incidenten binnen de Landstede Groep coördineren

Directeuren van de eenheden/stichtingen en de directeuren/hoofden binnen de Serviceorganisatie & bestuursdienst (Proceseigenaar)
Binnen de organisatie zijn er verschillende processen, zoals ICT, HRM, administratie, onderwijs, et cetera. Op elk van deze processen is iemand verantwoordelijk om te bepalen op welke wijze het informatiebeveiligings- en privacy beleid binnen het proces wordt vormgegeven. Dit gebeurt door middel van het opstellen van richtlijnen, procedures en instructies.

Bij beveiligingsincidenten is de directeur of hoofd medeverantwoordelijk voor het goed afhandelen van het incident. Hij dient beschikbaar te zijn tot en met het moment dat het incident volledig is afgehandeld, dit om bij besluitvorming en opschaling de juiste keuzes te maken.

SERT-coördinator[2]
De SERT-coördinator is benoemd door de ICT-teamleider en opereert in diens opdracht. Hij is bevoegd om het isoleren van computersystemen of netwerksegmenten te gelasten.

Informatiemanagement
In een co creatie met de Functionaris Gegevensbescherming wordt door Informatiemanagement het informatiebeveiligings- en privacy (IBP) beleid opgesteld. Gezamenlijk borgen ze dat deze 2-jaarlijks wordt vastgesteld door het College van Bestuur.

Informatiemanagement (IM) adviseert over specifieke informatiebeveiligingsmaatregelen in projecten en bewaakt de consistentie van de maatregelen.

Interne Auditor
De Interne Auditor controleert de organisatie, processen, interne rapportages en de veiligheidssituatie op het gebied van de Informatiebeveiliging en Privacy (IBP) binnen Landstede Groep met het doel om de risico's te beperken of weg te nemen.

Functioneel beheerder
Op basis van de richtlijnen, procedures en instructies van de proceseigenaar en/of procesbeheerder voert de functioneel beheerder (FB) zijn of haar taken uit.

Indien er beveiligingsincidenten zijn binnen het informatiesysteem van de functioneel beheerder, verzorgt deze de communicatie met de desbetreffende leverancier.

Teamleider
Naleving van het informatiebeveiligings- en privacy beleid is onderdeel van de integrale bedrijfsvoering. Iedere teamleider heeft de taak om:

- Ervoor te zorgen dat zijn medewerkers op de hoogte zijn het informatiebeveiligings- en privacy beleid.
- Toe te zien op de naleving van het informatiebeveiligings- en privacy beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft.
- Periodiek het onderwerp informatiebeveiligings- en privacy onder de aandacht te brengen in werkoverleggen, beoordelingen, et cetera.
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligings- en privacy onderwerpen.

In het geval van nieuwe ontwikkelingen, kan een teamleider optreden als procesbeheerder. Hij draagt zorg voor alle PIOFACH-aspecten[3] binnen het proces en heeft hierdoor ook aandacht voor de informatiebeveiliging- en privacyaspecten pinnen het project.

Teamleider ICT & Informatiemanagement
De ICT-teamleider vormt een technische aanspreekpunt voor incidenten en informatiebeveiliging.

[2] *SERT = Security Emergency Response Team*
[3] PIOFACH (Personeel, Informatievoorziening, Organisatie, Financiën, Automatisering, Communicatie en Huisvesting) is een acroniem binnen de bedrijfsvoering waarmee alle relevante bedrijfsvoering elementen gebundeld zijn. Met behulp van PIOFACH-analyse kan de impact van een verandering binnen de organisatie worden bepaald.

Gebruikersondersteuner
De Gebruikersondersteuner (GBO) ondersteunt een team bij het uitvoeren van het bedrijfsproces en helpt bij het juist uitvoeren van het informatiebeveiligings- en privacy beleid.
De Gebruikersondersteuner is het eerste aanspreekpunt bij vragen rondom informatiebeveiligings- en privacy en speelt een prominente rol bij het coördineren van beveiligingsincidenten, die plaats vinden binnen het team.

ICT Coördinator
De ICT Coördinator ondersteunt een team bij de ICT-middelen die bij het uitvoeren van het bedrijfs-proces gebruikt worden. De ICT Coördinator verzorgt de communicatie met het team ICT/IM, indien de ICT-middelen onrechtmatig gebruikt worden en een mogelijke datalek veroorzaken.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in de folder Integriteit in de praktijk.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de medezeggenschap).

7. Controle en rapportage

7.1. Evaluatie

Dit informatiebeveiligings- privacy beleid wordt elk jaar getoetst en bijgesteld. Hierbij wordt rekening gehouden met

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent de Landstede Groep een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- privacy beleid wordt getoetst.

7.2. Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om de risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij de Landstede Groep het bewustzijn van de individuele medewerker voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. De Functionaris Gegevensbescherming is verantwoordelijk voor het bewustwordingsproces en ontwikkelt jaarlijks een campagne hiervoor.

7.2.1. Helpdesk

De Functionaris Gegevensbescherming en de IBP-coördinator bemannen samen de Helpdesk IBP. Op Connect, het samenwerkingsplatform van Landstede Groep, is een omgeving ingericht waar medewerkers terecht kunnen voor informatie, vragen en antwoorden.

7.3. Classificatie en risicoanalyse

Bij de Landstede Groep heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

7.4. Incidenten en datalekken

In eerste instantie is de signalering en rapportage van een datalek een taak van het organisatie-onderdeel waar het lek heeft plaatsgevonden.

	INTERN	**EXTERN**
1	Een student of leerling meldt het incident bij zijn docent en/of coach. Een medewerker (*ook indien deze door een student of leerling is ingelicht*) meldt het incident bij de voor hem bekende functionaris op locatie (GBO'er, ICT-coördinator).	Een leverancier meldt het incident bij de Functioneel Beheerder van het desbetreffende informatiesysteem.
2	De GBO'er of ICT- coördinator verzamelt zoveel mogelijk informatie over het incident en bepaalt op basis van deze informatie of het incident gemeld moet worden. Dit doet hij bij:	De Functioneel Beheerder meldt het incident altijd bij:
3	a. SERT (Security Emergency Response Team) Door gebruik te maken van het algemene e-mailadres: **sert@landstede.nl** kan het incident gemeld worden. b. Directie desbetreffende organisatieonderdeel De directie is medeverantwoordelijk voor het goed afhandelen van het incident. Hij dient beschikbaar te zijn tot en met het moment dat het incident volledig is afgehandeld, dit om bij besluitvorming en opschaling de juiste keuzes te maken.	
4	Het SERT (Security Emergency Response Team) pakt na binnenkomst het incident zo snel mogelijk op. Gezamenlijk wordt gekeken hoe het incident afgehandeld moet worden. Het SERT bestaat uit de SERT-coördinator, de IBP-coördinator en de Functionaris Gegevens-bescherming. **SERT-coördinator** De SERT-coördinator bevoegd om (gedeelten) van computersystemen of netwerk-segmenten te isoleren. **IBP-Coördinator** De IBP-coördinator heeft een coördineren rol binnen het SERT. Hij communiceert met alle betrokken partijen en stelt iedereen ervan op de hoogte als het incident afgehandeld is. Het incident is pas afgehandeld, als de GBO'er/ICT-coördinator, de Functioneel Beheerder en de directeur ingelicht zijn. **Functionaris Gegevensbescherming** De functionaris Gegevensbescherming meldt, indien nodig, het incident bij de Autoriteit Persoonsgegevens.	

7.5. Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het informatiebeveiliging en privacy proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in het geval van tekortkomingen.

Met behulp van een jaarlijkse planning en control cyclus, wordt onder andere de inhoud en effectiviteit van het informatiebeveiligings- privacy beleid getoetst.
De IBP-coördinator voert periodiek audits uit. De Functionaris Gegevensbescherming heeft hierbij een adviserende rol. Op basis van deze audits wordt een verbetervoorstel gedaan richting:

- Een eenheid: Indien een aantal zaken niet op orde zijn, die alleen voor desbetreffende eenheid van toepassing zijn.
    - De directeur van de eenheid is zelf verantwoordelijk om deze zaken op te pakken en te verbeteren.
- Het CvB: Indien ernstige tekortkomingen geconstateerd worden, die voor de gehele Landstede Groep van toepassing zijn.
    - Binnen de besluitvorming wordt bepaald of en hoe het verbetervoorstel uitgevoerd gaat worden.
    - Nieuwe ontwikkelingen worden via de lijn of projectmatig uitgevoerd of geïmplementeerd.

7.6. Klachten

Klachten die een medewerker, leerling en student (betrokkene) heeft rondom zijn of haar privacy kunnen gemeld worden door gebruik te maken van het Protocol klachtenbehandeling Landstede Groep. Binnen dit protocol zijn procedures beschreven om de rechten van de betrokkene te borgen en de klacht af te handelen. Het betreft de volgende rechten:

- Recht op informatie
- Recht op inzage in en correctie van de persoonsgegevens
- Recht op verwijdering van de persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen
- Recht van verzet tegen verwerking van persoonsgegevens bij de grondslag gerechtvaardigd belang, of verzet tegen direct marketing en profilering
- De betrokkene heeft het recht om bij toestemming, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (granulaire toestemming).
- De betrokkene heeft het recht dat verbeteringen, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt
- Het recht op ‘bevriezing van de verwerking’ van zijn gegevens
- De betrokkene heeft het ‘recht om te worden vergeten’ door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting
- Recht op melding datalek: bij een datalek heeft de medewerker recht om daarover geïnformeerd te worden indien zij daar een zwaarwegend belang bij hebben

Bijlage A: Reglementen

In onderstaande tabel zijn alle reglementen opgenomen, die van toepassing zijn binnen de Landstede Groep. De documenten zijn los van dit beleid vastgesteld.

NR	NAAM
1	Privacyreglementen
2	Geautomatiseerde bewaking van publiek toegankelijke ruimtes
3	Sociale media voor leerlingen, studenten en cursisten
4	Sociale media voor medewerkers
5	Gedragscode gebruik bedrijfsmiddelen
6	Uitwisseling leer- en begeleidingsgegevens
7	Integriteit in de praktijk

Bijlage B: Beleidsregels en protocollen

In deze bijlage zijn de beleidsregels en protocollen beschreven die door de Landstede Groep gehanteerd worden.

Informatiebeveiliging

B1 Wachtwoord beleid

Omschrijving
Binnen Landstede Groep hanteren we een wachtwoord beleid. Dit beleid komt overeen met de Best Practices van Microsoft.
Binnen het beleid maken we onderscheid tussen verschillende typen gebruikers:

- Deelnemers, bestaande uit studenten, leerlingen en cursisten.
- Medewerkers.
- Service accounts

Deelnemers.
Voor deelnemers geldt een minder zwaar beleid omdat zij in principe niet bij gevoelige systemen kunnen komen. Dit is afgevangen door de Role-based Access Control (RBAC). Omdat deelnemers veel in de cloud werken, met Bring-Your-Own-Devices (BYOD's) is het voor hen lastig om een trigger te krijgen om hun wachtwoord aan te passen.

Medewerkers.
Voor medewerkers geldt een zwaarder beleid omdat zij wel op Landstede Groep systemen werken. Veel applicaties staan in de cloud, maar worden ontsloten via Single-Sign-On (SSO) en Active Directory Federation Services (ADFS). Voor een aantal applicaties geldt dat deze binnen de applicatie is voorzien van Multi-Factor Authenticatie (MFA).

Service Accounts.
Service accounts zijn account bedoeld voor het uitvoeren van bepaalde diensten, of het toegang hebben tot bepaalde data. Deze accounts worden aan service gekoppeld zodat de betreffende service toegang heeft tot de resources. Het beleid is hierdoor anders dan bij medewerkers en deelnemers. Zo is het wachtwoord meer complex, random gegenereerd, maar hoeft niet te worden gewijzigd naar een bepaalde periode, omdat anders de service omvalt.

Instellingen wachtwoorden.

Regels	Deelnemer	Medewerker	Service Accounts
Enforce password history	2	2	2
Maximum password age	180	180	180
Minimum password age	0	0	0
Minimum password length	8 characters	8 characters	16 characters random upper, lower, digits and special characters
Complexity	Enabled	Enabled	Enabled
Store reversable encryption	Disabled	Disabled	Disabled
Account lockout duration	5 minutes	5 minutes	5 minutes
Account lockout threshold	10 invalid logon attempts	10 invalid logon attempts	never
Reset account lockout counter after	5 minutes	5 minutes	5 minutes
Enforce user login restrictions	Enabled	Enabled	Enabled
Maximum lifetime for service ticket	600 minutes	600 minutes	600 minutes
Maximum lifetime for user tickets	10 hours	10 hours	10 hours
Maximum lifetime for ticket renewal	7 days	7 days	7 days
Maximul tolerance for computer clock synchronization	5 minutes	5 minutes	5 minutes

B2 – Beleid voor beveiligde inlogprocedures.

Er wordt gebruik gemaakt van landelijk geaccepteerde inlogprocedures.

- Voor cloudsystemen logt men in via
  - Active Directory Federation Services (ADFS) van Microsoft.
  - Magister voor docenten en leerlingen van het voortgezet onderwijs.
- Voor lokale systemen moet men zich aanmelden via Domain controllers.

Voor het inloggen wordt gebruik gemaakt van een gebruikersnaam en wachtwoord.
De gebruikersnaam wordt bepaald door Landstede Groep. Het wachtwoord is in beheer bij de gebruiker zelf. Voor het wachtwoord heeft Landstede Groep minimale eisen gesteld. Het wachtwoord mag tijdens het intikken niet zichtbaar zijn.

Inloggen via Multi Factor Authenticatie (MFA) is verplicht voor

- Beheerders van de belangrijkste informatiesystemen.
- Toegang tot bijzondere persoonsgegevens.

B3 - Beleid voor toegang tot netwerken en netwerkdiensten.

Een netwerkgebruiker wordt binnen Landstede Groep geregistreerd in een bronsysteem.
In deze bronsystemen is geregistreerd welke rol de netwerkgebruiker heeft binnen Landstede Groep en op welke plaats in de organisatiestructuur de werkzaamheden worden verricht.
Aan de hand van de registratie, de rol en de plaats in de organisatie worden rechten toegekend aan de netwerkgebruiker. Als een gebruiker meer rechten nodig heeft, wordt dat aangevraagd bij de ICT-coördinator die de benodigde rechten toekent. Jaarlijks worden de extra toegekende rechten gereviewd en aangepast als dit nodig is.

Daarnaast is er toegang geregeld voor leveranciers van informatiesystemen. Deze zijn nodig om de systemen goed in te richten en te monitoren. Dit valt onder de contracten met de leveranciers.

B4 Clear Screen beleid

De hoofdelementen van het 'clear screen' beleid zijn:

- Deze regels hebben zowel betrekking op vaste computerapparatuur (desktop), als op mobiele computerapparatuur (laptop, tablet, smartphone, etc.).
- Een computer mag nooit onbeveiligd en onbeheerd worden achtergelaten wanneer de gebruiker de werkplek verlaat. Wanneer de gebruiker de werkplek verlaat moet de gebruiker het scherm van de computer altijd beveiligen (ook wel omschreven als 'locken').
- Een computer wordt altijd voorzien van wachtwoordbeveiliging. Uitzonderingen op de standaard screensaver kunnen via Dienst Organisatieondersteuning, team ICT & Informatiemanagement worden aangevraagd en wordt beoordeeld door de het Security Emergency Response Team (SERT).
- Vertrouwelijke informatie mag nooit onbeveiligd en onbeheerd op een computer aanwezig zijn, waardoor derden toegang kunnen krijgen tot de computer en tot vertrouwelijke informatie.
- Wanneer een medewerker of student een computer onbeheerd en onbeveiligd aantreft, moet deze persoon direct actie ondernemen, door de verantwoordelijke voor deze computer te waarschuwen of door het scherm van de computer te beveiligen.

B5 Clear Desk beleid

De hoofdelementen van het 'clear desk' beleid zijn:

- Vertrouwelijke informatie mag niet onbeheerd en onbeveiligd op een werkplek aanwezig zijn wanneer de gebruiker de werkplek verlaat. Dit kan zijn in papieren vorm of op een mobiele informatiedrager, zoals een laptop, tablet of smartphone, etc.
- Onder de 'werkplek' op locatie valt naast het bureau van een individuele medewerker ook secretariaat, docentenkamer, postvakjes op de gang, publicatieborden, afvalbakken voor (tijdelijke) afvoer van papierafval, etc. Ook op deze plaatsen mag vertrouwelijke informatie niet zonder toezicht en controle toegankelijk zijn voor derden. Van belang is dat een 'werkplek' niet beperkt is tot de locaties van Landstede Groep, maar dat ook andere ruimtes als werkplek kunnen dienen, zoals de trein, een openbare kantoorplek of thuis.
- Bijzondere aandacht is vereist voor plaatsen waar vertrouwelijke informatie wordt uitgeprint en uitgewisseld, zoals bij printers, faxmachines, postvakken, etc.
- Vertrouwelijke informatie moet afgesloten worden bewaard wanneer de werkplek is verlaten, hetzij door de ruimte op een passende wijze af te sluiten (indien mogelijk), hetzij door de informatie in een afgesloten bureau of kast te bewaren.
- Wanneer een medewerker vertrouwelijke informatie onbeheerd aantreft, moet deze persoon direct actie ondernemen, door de verantwoordelijke voor de informatie en/of de werkplek te waarschuwen of door de vertrouwelijke informatie in veiligheid te stellen.

Privacy

B6 Verwerking van bijzondere persoonsgegevens

Artikel 1.

De instelling verwerkt geen persoonsgegevens betreffende:

- iemands religieuze of levensbeschouwelijke overtuigingen, *tenzij* dit gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag strikt noodzakelijk is,

- etnische afkomst, *tenzij* de instelling daartoe op grond van een wet verplicht is, of alleen in met het doel om personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen om feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen,

- biometrische gegevens (zoals vingerafdruk of irisscan) voor zover deze gebruikt worden met het oog op de unieke identificatie van een persoon,

- gezondheid of iemands seksueel gedrag of seksuele gerichtheid, voor zover dat met het oog op de speciale begeleiding van deelnemers of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is, *tenzij* de deelnemer voor het gebruik van deze categorieën persoonsgegevens zelf toestemming heeft gegeven voor het verwerken van de hiervoor genoemde categorieën persoonsgegevens.