# ISO 27001:2013

## Informatiebeveiligingsbeleid

Extern

Utrecht 11 jan 2021
Betreft: Versie 3.2

## Inhoud

Pagina



## Review en versiebeheer

| Naam | Versie | Datum |
|---|---|---|
| Security Officer | 0.1 | 24-10-2016 |
| Security Officer | 1.0 | 25-10-2016 |
| Security Officers | 1.1 | 28-12-2017 |
| Security Officers | 2.0 | 24-01-2018 |
| Security Officer | 3.0 | 19-12-2019 |
| Security Officer | 3.1 | 30-11-2020 |
| Security Officer | 3.2 | 11-1-2020 |

## BEGRIPPENLIJST

| Begrip | Definitie/verklaring |
|---|---|
| | |
| **Beschikbaarheid** | Waarborgen dat bevoegde gebruikers wanneer dat nodig is toegang hebben tot informatie en aanverwante bedrijfsmiddelen. |
| **Calamiteit** | Een onvoorziene gebeurtenis die leidt tot ernstige schade. |
| **Datalek** | Een datalek wordt gedefinieerd als het opzettelijk of onopzettelijk vrijgeven van beveiligde informatie aan een onvertrouwd publiek. |
| **Imagoschade** | Bij imagoschade gaat het om de reputatie van Employee Performance Group (of Conclusion Holding) en Supplier/klant. Dit kan bijvoorbeeld ontstaan door een datalek bij een klant of supplier/klant, waarbij informatie uit een systeem van Employee Performance Group in verkeerde handen is geraakt. |
| **Incident** | Onvoorziene gebeurtenis, storend voorval |
| **Integriteit** | Het waarborgen van de nauwkeurigheid en volledigheid van informatie en van de methoden waarmee informatie wordt verwerkt. |
| **LMS** | Learning Management System. De producten die worden geleverd en gehost door Employee Performance Group, met eventuele dienstverlening. |
| **Vertrouwelijkheid** | Waarborgen dat informatie alleen toegankelijk is voor degenen die daartoe geautoriseerd zijn. |

# 1. INLEIDING

Voor u ligt het Informatiebeveiligingsbeleid van Employee Performance Group B.V. (EPG), handelend onder de naam Conclusion Learning Centers (CLC). CLC is onderdeel van Conclusion, de meest veelzijdige zakelijke dienstverlener van Nederland. Als multidisciplinaire dienstverlener biedt Conclusion Learning Centers Integrale Learning & Development (L&D) oplossingen om organisaties volledig te ontzorgen bij het innoveren, ontwikkelen en beheren van het opleidingenproces. Het werkdomein wordt ingevuld vanuit de opvatting dat leerinterventies niet op zichzelf staan. Alleen door een integrale benadering van opleidingsvraagstukken vanuit verschillende disciplines kan L&D een duurzaam en verankerd onderdeel van de organisatie worden.

Voor de klanten van CLC is het van essentieel belang dat de bedrijfsvoering en met name de ICT-dienstverlening goed en betrouwbaar verloopt. Een goede ICT-beheersing is daarbij een voorwaarde om te kunnen blijven beschikken over een ICT-infrastructuur die voldoet aan de kwaliteitseisen op het terrein van wet- en regelgeving, beschikbaarheid, vertrouwelijkheid en integriteit. Om dit te bereiken maakt CLC gebruik van een beheer kader dat gebaseerd is op het normenkader voor informatiebeveiliging ISO27001:2013 en best practices uit de ISO27002.

Het beheerkader met de daarin opgenomen beheersmaatregelen is zoveel mogelijk vastgelegd in de door CLC ontwikkelde processen en procedures.

In deze veranderde samenleving waar door de vergaande digitalisering erg makkelijk informatie wordt uitgewisseld, is het belangrijk om als organisatie maatregelen te nemen om misbruik te voorkomen. CLC heeft een informatiebeveiligingsbeleid voor intern en extern gebruik opgesteld. Dit document beschrijft het externe gerichte informatiebeveiligingsbeleid. Wij vragen van onze Suppliers en klanten om zich hieraan te conformeren.

## 2. WAT IS INFORMATIEBEVEILIGING?

Informatiebeveiliging is het onderhouden en treffen van beleid, maatregelen, richtlijnen en procedures voor informatie en informatiesystemen ter bescherming van bedreigingen die van invloed kunnen zijn op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie, om de schade die door die bedreigingen kunnen ontstaan te minimaliseren.

a. Beschikbaarheid: Het LMS en relevante dienstverlening dienen op vooraf afgesproken locatie en tijdstip beschikbaar te zijn voor degene die daartoe geautoriseerd zijn.
b. Integriteit: Informatie op de klantportalen moet correct worden weergegeven en worden gewijzigd.
c. Vertrouwelijkheid: (Persoons) informatie is alleen toegankelijk voor geautoriseerde personen.

Employee Performance Group (EPG) realiseert zich dat ze dagelijks in haar dienstverlening te maken heeft met (persoons-) informatie van haar klanten. De supplier/klant van EPG dient zich ervan bewust te zijn dat zorgvuldige bewerking van (persoons) informatie van klanten een essentieel onderdeel is van de dienstverlening.

EPG heeft haar risico's met betrekking tot informatiebeveiliging in kaart gebracht. In de gevallen waarin de kans groot is dat door een incident schade ontstaat, implementeert EPG daar effectieve en efficiënte maatregelen implementeren die passen binnen haar beleid.

## 3. GEDRAGSCODE

Onderstaande gedragsregels zijn van groot belang tijdens het bewerken van persoonsgegevens.

I. Supplier/klant gebruikt alle persoonsgegevens strikt vertrouwelijk en in overeenstemming met de geldende wet- en regelgeving inzake de bescherming van persoonsgegevens.

II. Supplier/klant verplicht zich om personen die door haar worden ingezet bij de uitvoering van de overeenkomst dezelfde verplichtingen op te leggen als in het eerste lid van dit artikel zijn opgenomen.

III. Supplier/klant zal alle informatie in de ruimste zin des woords omtrent Employee Performance Group, de Opdrachtgevers van Employee Performance Group, de medewerkers van Employee Performance Group, de medewerkers van Opdrachtgevers van Employee Performance Group en de strategieën van Employee Performance Group strikt vertrouwelijk behandelen.

IV. Supplier/klant zal deze informatie tijdens de duur van deze overeenkomst en na het einde daarvan nimmer zonder schriftelijke toestemming van Employee Performance Group openbaar maken, aan derden ter inzage of in gebruik geven, of ten behoeve van derden gebruiken.

V. Supplier/klant zorgt ervoor dat haar medewerkers, consultants en andere bij de overeenkomst betrokken stakeholders van Supplier/klant, een geheimhoudingsverklaring zullen tekenen voorafgaand aan inschakeling voor een Opdrachtgever van Employee Performance Group, ofwel door een eigen geheimhoudingsverklaring van Supplier/klant die geldt als algehele gedragsregel voor medewerkers van Supplier/klant.

VI. Supplier/klant dient in het geval van een datalek direct een melding te maken bij Employee Performance Group via service.clc@conclusion.nl.

VII. Supplier/klant dient zich te conformeren aan het informatiebeveiligingsbeleid van Conclusion.

## 4. MINIMALE BEVEILIGINGSMAATREGELEN

EPG verwacht van haar Suppliers/klanten dat zij minimale beveiligingsmaatregelen hebben genomen om te kunnen voldoen aan de toepasselijke en algemeen aanvaarde beveiligingsstandaarden.

De te nemen beveiligingsmaatregelen zijn daarom ten minste de volgende:

- geïmplementeerd beveiligingsbeleid en het periodiek updaten en implementeren van het geüpdatet beveiligingsbeleid;
- geïmplementeerde gedragscode;
- geheimhoudingsverplichtingen in arbeidscontracten;
- veilige wijze voor het opslaan van gegevensbestanden;
- logische toegangscontroles door middel van kennis, zoals password of persoonlijke toegangscodes;
- logische toegangscontroles door middel van fysieke toegangsmiddelen, zoals een beveiligingspas;
- controleren van toegekende rechten;
- logging en controle van toegang tot het systeem (waaronder begrepen het controleren op tekenen van onrechtmatige toegang tot de Persoonsgegevens);
- herstelprocedures;
- encryptie van Persoonsgegevens tijdens elektronische overdracht naar externe partijen;
- voldoen aan de geheimhoudingsbepaling van de overeenkomst; en
- het aanwijzen van een beperkt aantal personen, die met de uitvoering van de Verwerking van Persoonsgegevens zijn belast en geautoriseerd zijn om zichzelf toegang te verlenen tot de Persoonsgegevens, welke personen uitdrukkelijk alleen gerechtigd zijn om de voor de uitvoering van de Overeenkomst noodzakelijke handelingen te verrichten.

## 5. MELDING EN AFHANDELING VAN SECURITY INCIDENTEN

Incidentbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door de supplier/klant gemeld wordt en de wijze waarop deze worden afgehandeld.

Het is van belang om te leren van security incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een goede informatie beveiligingsomgeving. Er is daarom een meldpunt (service.clc@conclusion.nl) ingericht bij de Servicedesk van EPG.

Supplier/klant is verantwoordelijk voor het signaleren van incidenten en inbreuken op informatiebeveiliging en zwakke plekken in de informatiebeveiliging. De supplier/klant is verplicht incidenten en inbreuken te melden bij EPG.

De incidenten worden afgehandeld en dienen als input voor de incident-rapportages. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen.

# 6. NALEVING

## 6.1 LIJNVERANTWOORDELIJKHEID

Supplier/klant zijn verantwoordelijk voor het naleven van de beveiligingseisen conform het informatiebeveiligingsbeleid. Supplier/klant spreken hun medewerkers aan in het geval van tekortkomingen.

Medewerkers die werken met vertrouwelijke en/of gevoelige informatie horen zich bewust te zijn van de verantwoordelijkheid die hierbij komt.

## 6.2 VERANDERINGEN IN DE DIENSTVERLENING

Veranderingen in de dienstverlening van supplier/klant, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kwaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.

Eventuele veranderingen dienen te worden gemeld bij de Servicedesk (service.clc@conclusion.nl) van EPG.

## 6.3 WET EN REGELGEVING

Onderstaand is aangegeven op wat voor wijze om wordt gegaan met relevante wet- en regelgeving:

**Algemene verordening gegevensbescherming**
Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De AVG zorgt onder meer voor:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

**Intellectueel eigendom / Auteurswet**
Employee Performance Group gaat zorgvuldig om met intellectuele eigendom van anderen. Eigen intellectuele eigendommen worden beschermt door passende IT maatregelen en door dit contractueel vast te leggen, waardoor een partij niet zomaar inbreuk kan maken op intellectuele eigendommen van Employee Performance Group.

**Wet Computercriminaliteit**
De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat “enige beveiliging” vereist is voordat er sprake kan zijn van eventuele strafrechtelijke vervolging van delicten jegens de organisatie.

**Wet identificatieplicht**
Iedereen dient zich te legitimeren wanneer dit van hem of haar wordt gevraagd. Bij overheidsinstanties is legitimeren te allen tijde nodig.

**Wet meldplicht datalekken**
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

## 7. AKKOORDVERKLARING

De directie van EPG stelt het informatiebeveiligingsbeleid vast en draagt dit beleid uit aan haar medewerkers en suppliers/klanten.

Namens de directie van EPG

Celine van Hulst

Datum 13 januari 2021 Handtekening 

**CONTACT**

Employee Performance Group BV
Postbus 85030
3508 AA  Utrecht
Nederland

T +31 (0)30 744 01 30
info@conclusionlearningcenters.nl
www.conclusionlearningcenters.nl