CONCLUSION
LEARNING CENTERS

ISO 27001:2013

Informatiebeveiligingsbeleid extern

Utrecht: 11 januari 2023
Versie: 3.6

Inhoud

Pagina

BEGRIPPENLIJST **4**

1. INLEIDING **5**

2. WAT IS INFORMATIEBEVEILIGING? **6**

3. GEDRAGSCODE **7**

4. MINIMALE BEVEILIGINGSMAATREGELEN **8**

5. MELDING EN AFHANDELING VAN SECURITY INCIDENTEN **9**

6. NALEVING **10**
6.1 LIJNVERANTWOORDELIJKHEID 10
6.2 VERANDERINGEN IN DE DIENSTVERLENING 10
6.3 WET EN REGELGEVING 10

7. AKKOORDVERKLARING **12**

Review en versiebeheer

Naam	Versie	Datum	Wijzigingen
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	Jaarlijkse review SO, MT
Security Officer	3.2	11-1-2021	Aanpassingen na review SO, MT
Security Officer	3.3	21-12-2021	Jaarlijkse review SO, MT
Security Officer	3.4	03-01-2022	Aanpassingen na review SO, MT
Security Officer	3.5	22-12-2022	Jaarlijkse review SO
Security Officer	3.6	05-01-2023	Aanpassingen na review MT

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 Conclusion Learning Centers (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 Conclusion Learning Centers 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 Conclusion Learning Centers, 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.

Conclusion Learning Centers helpt organisaties om leren en ontwikkelen in het hart van de organisatie te positioneren.
Met het Learning Management System (LMS) Class biedt CLC een digitaal leerplatform waarmee je eenvoudig leerervaringen voor medewerkers creëert, promoot en beheert. Stel leiders en leerexperts in staat om intuïtieve en waardevolle leercontent aan te bieden. Prikkel de nieuwsgierigheid van medewerkers om met leren bezig te zijn en zet leren centraal in de organisatie. Met verschillende modules en diensten richt CLC het leerlandschap op maat voor u in.

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 de beheersmaatregelen 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 klanten en leveranciers 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.

Conclusion Learning Centers (CLC) realiseert zich dat ze dagelijks in haar dienstverlening te maken heeft met (persoons-) informatie van haar klanten. De klant/leverancier van CLC dient zich ervan bewust te zijn dat zorgvuldige bewerking van (persoons) informatie van klanten een essentieel onderdeel is van de dienstverlening.

CLC 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 CLC 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. Klant/leverancier gebruikt alle persoonsgegevens strikt vertrouwelijk en in overeenstemming met de geldende wet- en regelgeving inzake de bescherming van persoonsgegevens.

II. Klant/leverancier 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. Klant/leverancier zal alle informatie in de ruimste zin des woords omtrent Conclusion Learning Centers, de Opdrachtgevers van Conclusion Learning Centers, de medewerkers van Conclusion Learning Centers, de medewerkers van Opdrachtgevers van Conclusion Learning Centers en de strategieën van Conclusion Learning Centers strikt vertrouwelijk behandelen.

IV. Klant/leverancier zal deze informatie tijdens de duur van deze overeenkomst en na het einde daarvan nimmer zonder schriftelijke toestemming van Conclusion Learning Centers openbaar maken, aan derden ter inzage of in gebruik geven, of ten behoeve van derden gebruiken.

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

VI. Klant/leverancier dient in het geval van een datalek direct een melding te maken bij Conclusion Learning Centers via service.clc@conclusion.nl.

VII. Klant/leverancier dient zich te conformeren aan het informatiebeveiligingsbeleid van Conclusion Learning Centers.

VIII. Klant/leverancier zal in afstemming met CLC een verwerkersovereenkomst ondertekenen en zich hieraan houden gedurende de duur van het contract. Wijzigingen in de verwerkersovereenkomst kunnen alleen met toestemming van beide partijen worden opgenomen.

4. MINIMALE BEVEILIGINGSMAATREGELEN

CLC verwacht van haar klanten/leveranciers 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 klant/leverancier 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 CLC.

Klant/leverancier is verantwoordelijk voor het signaleren van incidenten en inbreuken op informatiebeveiliging en zwakke plekken in de informatiebeveiliging. De klant/leverancier is verplicht incidenten en inbreuken te melden bij CLC.

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

Klant/leverancier is verantwoordelijk voor het naleven van de beveiligingseisen conform het informatiebeveiligingsbeleid. Klant/leverancier spreekt 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 klant/leverancier, 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 CLC.

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 privacy rechten;
- Meer verantwoordelijkheden voor organisaties;
- Dezelfde, stevige bevoegdheden voor alle Europese privacy toezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

Intellectueel eigendom/ Auteurswet
Conclusion Learning Centers gaat zorgvuldig om met intellectuele eigendom van anderen. Eigen intellectuele eigendommen worden beschermd door passende IT-maatregelen en door dit contractueel vast te leggen, waardoor een partij niet zomaar inbreuk kan maken op intellectuele eigendommen van Conclusion Learning Centers.

Wetboek van Strafrecht
Wetboek dat regelt welke delicten als een misdrijf en welke delicten als een overtreding worden beschouwd en welke soorten straffen daarvoor opgelegd kunnen worden.

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.

Mededingingswet
Er mag geen economische machtpositie worden genomen.

Arbo wet, ARBO besluit en ARBO-regeling
Regels om veiligheid, gezondheid en welzijn van de medewerkers. Alle bedrijven en medewerkers moeten zich houden aan de regels die deze wet stelt.

Wet op financieel toezicht
Regelt het toezicht op Nederlandse financiële instellingen.

De doelstellingen van de Wft zijn:
- Inzichtelijkheid
- Doelgerichtheid
- Marktgerichtheid.

Met de doelstelling van marktgerichtheid wordt eveneens getracht een bijdrage te leveren aan een verbeterde Nederlandse concurrentiekracht.

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).

Wet Beveiliging Netwerk- en Informatiesystemen
De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) is per 9 november 2018 in werking getreden. Deze wet regelt een meldplicht van incidenten en een zorgplicht (treffen van beveiligingsmaatregelen).

7. AKKOORDVERKLARING

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

Namens de directie van CLC

Celine van Hulst

Datum 11 januari 2023 Handtekening 

CONCLUSION
LEARNING CENTERS

CONTACT
Conclusion Learning Centers BV
Postbus 85030
3508 AA Utrecht
Nederland

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