CONCLUSION
LEARNING CENTERS

ISO 27001:2013

Informatiebeveiligingsbeleid extern

Utrecht: 24 januari 2018
Versie: 2.0

Inhoud

Pagina

Review en versiebeheer

Naam	Versie	Datum
Security Officer	0.1	24-10-2016
Security Officer	1.0	25-10-2016
Security Officers EPG	1.1	28-12-2017
Security Officers EPG	2.0	24-01-2018

BEGRIPPENLIJST

Begrip	Definitie/verklaring
Beschikbaarheid	Waarborgen dat bevoegde gebruikers wanneer dat nodig is toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
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.
Vertrouwelijkheid	Waarborgen dat informatie alleen toegankelijk is voor degenen die daartoe geautoriseerd zijn.

1. INLEIDING

Conclusion Learning Centers (CLC) is sinds 1 januari 2017 een handelsmerk van Employee Performance Group (EPG). De ISO27001:2013 certificering is behaald voor de dienstverlening van CLC m.b.t. het product Class.

Conclusion Learning Centers is marktleider in Learning Business Process Outsourcing (BPO) in Nederland. CLC verzorgt het totale proces van opleidingsaanvragen (inkoop, organisatie, planning administratieve afhandeling, facturatie en evaluatie) voor klanten volgens contractuele afspraken en SLA. Daarnaast levert CLC een Learning Management Systeem (LMS) genaamd Class.

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 Supplier/klant en klanten om zich hier aan 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: Informatie dient te allen tijde beschikbaar te zijn.
b. Integriteit: Informatie op de klantportalen moet correct worden weergegeven en worden gewijzigd.
c. Vertrouwelijkheid: (Persoons) informatie is alleen toegankelijk voor geautoriseerde personen.

CLC realiseert zich dat ze dagelijks in haar dienstverlening te maken heeft met (persoons-) informatie van haar klanten. Supplier/klant die een samenwerking met CLC aangaan, dienen zich 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, zal 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.

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

2. 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 en tweede lid van dit artikel zijn opgenomen.

3. Supplier/klant zal alle informatie in de ruimste zin des woords omtrent CLC, de opdrachtgevers van CLC, de medewerkers van CLC, de medewerkers van opdrachtgevers van CLC en de strategieën van CLC strikt vertrouwelijk behandelen. Supplier/klant zal deze informatie tijdens de duur van deze overeenkomst en na het einde daarvan nimmer zonder schriftelijke toestemming van CLC openbaar maken, aan derden ter inzage of in gebruik geven, of ten behoeve van derden gebruiken.

4. Supplier/klant zorgt ervoor dat haar medewerkers, consultants en andere bij de overeenkomst betrokkenstakeholders van supplier/klant, een geheimhoudingsverklaring zullen tekenen voorafgaand aan inschakeling voor een opdrachtgever van CLC, ofwel door een eigen geheimhoudingsverklaring van supplier/klant die geldt als algehele gedragsregel voor medewerkers van Supplier/klant.

5. Supplier/klant dient in het geval van een datalek direct een melding te maken bij CLC doormiddel van een incidentmelding via service.clc@conclusion.nl.

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

7. Supplier/klant deelt ontvangen persoonsgegevens niet met derden.

8. Supplier/klant gebruikt ontvangen persoonsgegevens niet voor reclame of marketing doeleinde.

9. Supplier/klant dient zich te conformeren aan het informatiebeveiligingsbeleid van CLC.

4. BELEIDSPRINCIPES TEN AANZIEN VAN MAATREGELEN

4.1 MEDEWERKERS ZIJN EEN ONMISBARE SCHAKEL

De informatiebeveiliging kan technisch en fysiek optimaal georganiseerd zijn, maar als medewerkers niet op de hoogte zijn van het informatiebeveiligingsbeleid en handelen op een onzorgvuldige wijze is de beveiliging niet waterdicht. Bewustwording is hierbij een belangrijk punt. Als alle medewerkers bewust zijn van het informatiebeveiligingsbeleid, dan kunnen de medewerkers hier op professionele en beveiligde manier mee omgaan.

4.2 FYSIEKE BEVEILIGING

Informatie hoort ook op een fysieke manier beveiligd te zijn. Als de toegankelijkheid naar een pand te openlijk is voor onbevoegden, dan is er zeker sprake van een informatiebeveiligingsrisico. Supplier/klant dienen rekening te houden met mogelijke verlies van data door bijvoorbeeld onbevoegd toegang door derden.

4.3 BEHANDELEN VAN MEDIA

4.3.1 BEHEER VAN GEGEVENSDRAGERS

Gegevensdragers mogen niet worden gebruikt voor het transporteren van persoonsgegevens ontvangen vanuit CLC.

4.3.2 BEHEER VAN APPARATUUR

Laptops of dergelijke apparatuur met persoonsgegevens vanuit CLC mogen niet onbeheerd worden achter gelaten in ruimtes.

4.3.3 OVERDRAGEN VAN FYSIEKE MEDIA

Er mag geen fysieke media overgedragen worden aan derden met persoonsgegevens ontvangen vanuit CLC.

4.4 ENCRYPTIE (VERSLEUTELING)

Opgeslagen persoonsgegevens dienen bewaard te worden op een omgeving/folder die beveiligd is met een encryptie. De encryptie dient versleuteld te worden met een veilig (sterk) wachtwoord.

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 CLC.

Supplier/klant zijn 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 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

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 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:

Wet Bescherming Persoonsgegevens (vervalt 25 mei, met ingang van de AVG)
Conclusion Learning Centers heeft technische en organisatorisch maatregelingen genomen om aan de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) te voldoen. Naleving van de beveiligingsmaatregelen leidt tot voldoen aan de wet.

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 Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. 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
Conclusion Learning Centers 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 Conclusion Learning Centers.

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 ten alle tijde nodig.

Wet meldpunt 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 Supplier/klant.

Namens de directie van EPG

Celine van Hulst

Utrecht, 15 februari 2018 Handtekening

CONCLUSION
LEARNING CENTERS

CONTACT
Employee Performance Group BV
Postbus 85030
3508 AA Utrecht
Nederland

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