

CONCLUSION **LEARNING CENTERS**



ISO 27001:2013

Informatiebeveiligingsbeleid

Utrecht: 15 januari 2018
Versie: 4.0

Inhoud	Pagina
BEGRIPPENLIJST	3
1. INLEIDING	4
2. WAT IS INFORMATIEBEVEILIGING?	5
3. DOELSTELLINGEN EN UITGANGSPUNTEN CLC	6
4. ROLLEN, VERANTWOORDELIJKHEDEN EN GOVERNANCE	7
4.1 ROLLEN EN VERANTWOORDELIJKHEDEN	7
4.2 GOVERNANCE	8
5. WET- EN REGELGEVING	10
6. BELEIDSPRINCIPES TEN AANZIEN VAN MAATREGELEN	12
6.1 MEDEWERKERS ZIJN EEN ONMISBARE SCHAKEL	12
6.2 FYSIEKE BEVEILIGING	12
6.3 VEILIGE BEDIENING VAN IT VOORZIENINGEN	12
6.4 CONTINUÏTEITSMANAGEMENT	12
7. MELDING EN AFHANDELING VAN SECURITY INCIDENTEN	13
8. NALEIVING	14
8.1 LIJNVERANTWOORDELIJKHEID	14
8.2 AUDITS	14
9. AKKOORDVERKLARING	15

Review en versie beheer

Functie	Versie	Datum
Security Officer	0.8	22-01-2015
Consultant Deloitte	0.9	22-02-2015
Directeur	1.0	23-02-2015
Auditor DNV	1.0	26-02-2015
Security Officer	2.0	27-07-2015
Directeur	2.0	28-07-2015
Security Officer	2.1	08-10-2015
Security Officer	3.0	09-10-2015
Security Officer	3.1	20-10-2015
Security Officer	3.2	07-07-2016
Security Officer	3.3	09-09-2016
Security Officer	3.4	23-11-2016
Security Officer	3.5	28-12-2017
Security Officer	4.0	15-01-2018

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 opgesteld. Het beleid wordt in dit document weergegeven.

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 Class systeem 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.

CLC realiseert zich dat ze dagelijks in haar dienstverlening te maken heeft met (persoons-) informatie van haar klanten. De medewerkers van CLC zijn zich ervan bewust 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. DOELSTELLINGEN EN UITGANGSPUNTEN CLC

Dit document bevat de basis doelstelling en uitgangspunten van CLC op het gebied van informatiebeveiliging. Er zijn voor diverse deelgebieden zoals incidentmanagement, toegangsbeveiliging etc. eveneens doelstellingen en uitgangspunten opgesteld, deze zijn te vinden in betreffende documenten over de deelgebieden.

De onderstaande doelstellingen worden door CLC gebruikt voor het Information Security Management System (ISMS).

- Er vinden 0 security calamiteiten per jaar plaats, die betrekking hebben tot fraude, datalekken en langdurige uitval (langer als 4 uur) van het Learning Management System (Class).
- De organisatie heeft minimaal fase 3 (volledige bewustwording vanuit de organisatie) security volwassenheid volgens het security model van Stacey.
- Het behalen en behouden van de ISO27001 certificaat voor CLC en hiermee voldoen aan de eisen die dit certificaat stelt.
- Minimaal één keer in de 12 maanden zullen er Attack en Penetration testen worden uitgevoerd om de beveiliging van het Learning Management System te waarborgen.

De volgende uitgangspunten met betrekking tot informatiebeveiliging zijn door de directie van CLC goedgekeurd.

1. Directie en de teamleads van EPG zijn primair verantwoordelijk voor het informatiebeveiligingsbeleid. Zij dienen dit beleid toe te passen in de keuzes die ze maken en uit te dragen richting de organisatie en haar stakeholders.
2. Informatiebeveiliging is een verantwoordelijkheid van alle medewerkers van CLC. Alle medewerkers moeten op de hoogte worden gebracht van het informatiebeveiligingsbeleid, geldende gedragscodes etc. Alle medewerkers zijn verplicht jaarlijks deel te nemen aan Awareness activiteiten m.b.t. informatiebeveiliging.
3. Informatiebeveiligingsincidenten dienen op een zorgvuldige en correcte manier te worden opgepakt. De afhandeling van beveiligingsincidenten dient volgens de daarvoor vastgestelde procedures te worden uitgevoerd.
4. De bestaande en nieuwe procedures en maatregelen worden getoetst aan de relevante wet- en regelgeving. Door het toepassen van beveiligingsmaatregelen voldoet CLC aan de relevante wetgeving waaronder de Algemene Verordening Gegevensbescherming (AVG).
5. Jaarlijkse controle op wet- en regelgeving m.b.t. informatiebeveiliging.
6. Informatiebeveiliging is een continue doorlopend proces. Jaarlijks zal het beleid worden herzien en er zal een risicobeoordeling en een interne en externe audit plaatsvinden. Op deze manier wordt gecontroleerd of het informatiebeleid van CLC nog voldoende waarborgen biedt.

4. ROLLEN, VERANTWOORDELIJKHEDEN EN GOVERNANCE

4.1 ROLLEN EN VERANTWOORDELIJKHEDEN

Voor het handhaven van het informatiebeveiligingssysteem is een security officer aangesteld. Naast de security officer zijn er nog een aantal andere functies die taken en verantwoordelijkheden hebben met betrekking tot informatiebeveiliging.

a. Directie EPG is eindverantwoordelijke. Daarmee geeft zij richting aan het informatiebeveiligingsbeleid en systeem en draagt dit uit richting de organisatie. De directie is betrokken bij het proces, erkent zich in het beleid en is belast met het toekennen van verantwoordelijkheden en budget (voor het implementeren van de beheersmaatregelen) met betrekking tot informatiebeveiliging.

b. Teamleads zijn verantwoordelijk voor de naleving van het informatiebeveiligingsbeleid en het implementeren van informatiebeveiligingsmaatregelen binnen zijn of haar afdeling/proces.

c. Security officer is verantwoordelijk voor het opzetten en de aansturing van het informatiebeveiligingssysteem. Daarbij wordt direct gerapporteerd aan de directie.

d. Medewerkers zijn de gebruikers van de (klant)informatie en Class. Zij zijn verplicht de regels met betrekking tot het beveiligen van Class, omgang en verwerken van (klant) informatie en regels aangaande bedrijfsmiddelen op te volgen.

Functie	Strategisch (plannen)	Tactisch (aansturing)	Operationeel (uitvoering)
a. Directie EPG	<ul style="list-style-type: none"> - Goedkeuren en uitdragen informatiebeveiligingsbeleid en informatiebeveiligings-systeem. - Beschikbaar stellen van budget en resources voor de implementatie van beveiligingsmaatregelen 	<ul style="list-style-type: none"> - Aansturen van de security officer - Initiëren van interne en externe audits. - Toezicht houden op informatiebeveiliging 	<ul style="list-style-type: none"> - Naleven van informatiebeveiligingsbeleid en de informatiebeveiligingsmaatregelen
b. Teamleads	N.v.t.	<ul style="list-style-type: none"> - Implementeren specifieke informatiebeveiligingsmaatregelen voor de eigen afdeling/proces. - Aansturing van medewerkers - Toezicht houden op naleving van informatiebeveiligingsbeleid en maatregelen door zijn/haar medewerkers. <p><u>Specifiek voor de Product owner Class</u></p> <ul style="list-style-type: none"> - Owner van de Class applicatie 	<ul style="list-style-type: none"> - Uitvoeren van self assessments - Rapporteert aan de security officer aangaande incidenten, kwetsbaarheden, wijzigingen, verbeteringen op het gebied van informatiebeveiliging - Naleven van informatiebeveiligingsbeleid en de informatiebeveiligingsmaatregelen <p>Specifiek voor de Product Owner Class :</p> <ul style="list-style-type: none"> - signaleert kwetsbaarheden in Class t.a.v. informatiebeveiliging - toetst nieuwe functionaliteiten en

			technische ontwerpen aan het informatie-beveiligingsbeleid en relevante wet- en regelgeving
c. Security officer	<ul style="list-style-type: none"> - Opstellen informatie-beveiligingsbeleid - Opstellen informatie-beveiligingssysteem 	<ul style="list-style-type: none"> - Ondersteunen en uitvoeren van interne audits. - Ondersteunen bij en coördineren van externe audits - Coördineren bewustwordingsproces - Bewaken van het informatiemanagementsysteem 	<ul style="list-style-type: none"> - Rapporteren status informatiebeveiliging aan de directie - Meldpunt voor afwijkingen, incidenten en verbeteringen m.b.t. informatiebeveiligingsbeleid - Naleven van beveiligingsmaatregelen en- beleid. - Kan in het geval van een groot risico (volgens een risicoanalyse) systemen onderbreken.
d. Medewerkers	N.v.t.	N.v.t.	<ul style="list-style-type: none"> - Naleven van informatiebeveiligingsbeleid en de informatie-beveiligingsmaat-regelen <p><u>Specifiek voor de Class architect:</u></p> <ul style="list-style-type: none"> - rapporteert aan de security officer aangaande incidenten, kwetsbaarheden, wijzigingen, verbeteringen op het gebied van informatiebeveiliging

4.2 GOVERNANCE

Het informatiebeveiligingssysteem is een continu doorlopend proces welke periodiek wordt gecontroleerd aan de hand van de in het systeem opgenomen controle methodieken. Jaarlijks wordt er een businessplan opgesteld met o.a. doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging. Tijdens het jaarlijkse overleg met het MT wordt het informatiebeveiligingsbeleid herzien. Nieuw beleid wordt ontwikkeld volgens de procedure 1.1 beleid ontwikkelen opgenomen in het handboek.

Security overleg	
Doel	Bespreken incidenten, verbeterpunten, interne audit, periodieke controles
Wie	Security officer, Procesmanager/Kwaliteitsmanager
Agenda	<ul style="list-style-type: none"> - Bespreken vorige notulen - Periodieke controle op gebruiker accounts (rollen, rechten en uitdiensttreding) - Openstaande bevindingen vanuit audits/overleggen - Verbeterpunten vanuit de organisatie
Frequentie	Elke maand

Management Review	
Doel	Bespreken jaarplan, verbeterpunten, risicoanalyse
Wie	Security officer, Lead .Net Developers, Head Learning Services, Head Learning Management, Procesmanager en Operational Manager
Agenda	<ul style="list-style-type: none"> - Vorige Management Review - ISMS governance en management <ul style="list-style-type: none"> o Goedkeuren en ondertekenen van het informatiebeveiligingsbeleid (IBB), intern en extern o Wet en regelgeving in IBB beoordelen o Geheimhoudingsverklaring beoordelen o SoA beoordelen o Grote veranderingen in het ISMS o Trends en prestatie van het ISMS - KPI's bespreken <ul style="list-style-type: none"> o Er vinden 0 security calamiteiten plaats, die betrekking hebben tot fraude, informatielekken en langdurige uitval (langer als 4 uur) van het Class systeem. o De organisatie heeft minimaal fase 3 (volledige bewustwording vanuit de organisatie) security volwassenheid volgens het security model van Stacey. o Het behalen en behouden van de ISO27001 certificaat en hiermee voldoen aan de eisen die dit certificaat stelt. o Minimaal één keer in de 12 maanden zullen er Attack en Penetration testen worden uitgevoerd om de beveiliging van het LMS te waarborgen. - ISMS verbeteringen <ul style="list-style-type: none"> o Interne audit resultaten - Risicoanalyse <ul style="list-style-type: none"> o Top 19 risico's, zien wij nieuwe risico's die belangrijk zijn te vermelden? - Crisis Management Plan <ul style="list-style-type: none"> o Is het plan nog realistisch? o Inplannen van het testen - WVTTK
Frequentie	Minimaal twee keer per jaar

5. 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 maatregelen 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.

Mededingingswet

Er mag geen economische machtspositie 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 de 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 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).

6. BELEIDSPRINCIPES TEN AANZIEN VAN MAATREGELEN

6.1 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.

6.2 FYSIEKE BEVEILIGING

Informatie hoort ook op een fysieke manier beveiligd te zijn. Als de toegankelijkheid naar de locaties te openlijk is voor onbevoegden, dan is er zeker sprake van een informatiebeveiligingsrisico. Bij binnenkomst van het pand zal de receptie controles uitvoeren op onbekende bezoekers. Hiermee wordt de directe toegang tot de locaties beschermt, tevens is toegang alleen mogelijk met een druppel of pas. Dit dient als een sleutel voor de locaties en hiermee kan toegang worden verleend. Zonder de druppel of pas kan alleen de receptie een bezoeker toegang geven tot de locaties.

6.3 VEILIGE BEDIENING VAN IT VOORZIENINGEN

Via IT netwerken wordt veel informatie verspreid. Deze netwerken horen veilig bediend en beheerd te worden. Interne netwerken worden beheerd door Conclusion FIT (zie overeenkomst met Conclusion FIT). Bescherming tegen virussen en ongewenste e-mail valt hier ook onder.

Naast het beheer van de netwerken is het ook uitermate belangrijk dat er met zorg en veiligheid gebruik van wordt gemaakt van de netwerk mogelijkheden. Medewerkers zullen bewust moeten zijn dat er geen gevoelige informatie gedeeld mag worden via e-mail.

6.4 CONTINUÏTEITSMANAGEMENT

Conclusion Learning Centers wil onderbrekingen in de bedrijfsvoering voorkomen en de kritische processen beschermen tegen gevolgen van omvangrijke storingen. Storingen kunnen onvoorziene calamiteiten zoals ernstige computerstoringen, brand of waterschade zijn. Het crisis management plan geeft inzicht in de acties die Conclusion Learning Centers zou nemen bij een betreffende calamiteiten van eerder genoemd formaat.

Naast het crisis management plan wilt Conclusion Learning Centers risico's gestructureerd identificeren, risico's verminderen en de consequenties bewerken van incidenten die schade kunnen toebrengen.

7. 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 medewerkers gemeld worden 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 ingericht bij de Servicedesk.

Alle medewerkers zijn verantwoordelijk voor het signaleren van incidenten en inbreuken op informatiebeveiliging en zwakke plekken in de informatiebeveiliging. De medewerker is verplicht incidenten en inbreuken te melden bij zijn of haar directe leidinggevende of bij de Servicedesk.

De incidenten worden door de medewerkers zelf geregistreerd in de Servicedesk. De incidenten worden afgehandeld en dienen als input voor de incident-rapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen.

8. NALEVING

8.1 LIJNVERANTWOORDELIJKHEID

De managers van een betreffende afdeling zijn verantwoordelijk voor het naleven van de beveiligingseisen conform het informatiebeveiligingsbeleid. De managers spreken hun medewerkers aan in het geval van tekortkomingen en nemen hierbij de gepaste disciplinaire maatregelen.

Medewerkers die werken met vertrouwelijke en/of gevoelige informatie horen zich bewust te zijn van de verantwoording die hierbij komt. De Lead .net Developers en de Procesmanager waarborgen de autorisatiematrix (zie Handboek Kwaliteit en informatiebeveiliging: hoofdstuk 6.13.2), hierbij zorgen ze voor de juiste bevoegdheden per rol en bewaken hiermee de gegevensintegriteit van Class.

8.2 AUDITS

De werking van het informatiebeveiligingsbeleid wordt ook onafhankelijk beoordeeld. Dit wordt jaarlijks beoordeeld doormiddel van een interne audit vanuit Conclusion FIT en externe audit vanuit DNV-GL. Hierbij wordt er een Auditplan opgesteld waarbij wordt gekeken naar het waarborgen van het proces en de documentatie die dit proces ondersteunt. Zwakheden en risico's worden tijdens deze interne audit aangetoond en hier kunnen dan maatregelen voorgenomen worden.

Tevens worden er PEN testen (zie hoofdstuk 3) uitgevoerd op het Class systeem. Deze testen worden door een extern bedrijf uitgevoerd en zullen zwakheden en risico's aantonen in het Class systeem.

9. AKKOORDVERKLARING

De directie van EPG stelt het informatiebeveiligingsbeleid vast en draagt dit beleid uit aan haar medewerkers en controleert de uitvoering en het evaluatieproces.

Namens de directie van EPG

Celine van Hulst



Datum: 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