Verwerkersovereenkomst

Ingangsdatum: _____

Studytube biedt een online, geautomatiseerd systeem aan waarmee organisaties hun werknemers opleidingen, cursussen, trainingen en andere leervormen kunnen aanbieden, de voortgang van werknemers kunnen bijhouden en het opleidingsaanbod kunnen beheren. Om dit te doen zal Studytube Persoonsgegevens van deze werknemers moeten verwerken. Studytube zal daarbij optreden als Verwerker in de zin van de toepasselijke regelgeving en Klant als Verwerkingsverantwoordelijke. Deze Verwerkersovereenkomst bevat de voorwaarden waaronder Studytube voor Klant zal optreden als Verwerker en maakt als bijlage onlosmakelijk onderdeel uit van de Overeenkomst. Alle bepalingen van de Overeenkomst en van de Gebruiksvoorwaarden zijn onverkort van toepassing op deze Verwerkersovereenkomst, tenzij daarvan in deze Verwerkersovereenkomst wordt afgeweken.

Artikel 1 Definities en Interpretatie

1.1 In deze Verwerkersovereenkomst worden de volgende begrippen als volgt gedefinieerd:

AVG: de Europese Algemene Verordening Gegevensbescherming (2016/679).

Betrokkene: degene op wie een Persoonsgegeven betrekking heeft (art. 4 lid 1 AVG).

Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens (art. 4 lid 12 AVG).

Gebruiksvoorwaarden: de Studytube Gebruiksvoorwaarden voor klanten.

Klant: de partij die als Klant is aangeduid in de Overeenkomst.

Modules: de verschillende onderdelen van het Platform die door Klant worden afgenomen, zoals opgenomen in de Overeenkomst.

Overeenkomst: de overeenkomst tussen Studytube en Klant voor toegang en gebruik van het Platform.

Partijen: waar van toepassing, Studytube en/of Klant.

Persoonsgegevens: alle van Klant in het kader van het uitvoeren van de Overeenkomst verkregen informatie over een geïdentificeerde of identificeerbare Gebruiker (art. 4 lid 1 AVG).

Platform: het online, geautomatiseerde e-learning platform van Studytube waarop de Bedrijfsacademy voor Klant wordt geopend en ingericht, inclusief de Modules.

Studytube: de besloten vennootschap Studytube B.V., gevestigd te Amsterdam en ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 51290901.

Subverwerker: een derde partij die door Studytube wordt ingeschakeld om ten behoeve van Klant Persoonsgegevens te verwerken, zonder aan het rechtstreeks gezag van Studytube te zijn onderworpen.

Verwerker: degene die ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt zonder aan zijn rechtstreeks gezag te zijn onderworpen (art. 4 lid 8 AVG).

Verwerkersovereenkomst: deze verwerkersovereenkomst inclusief bijsluiters, alsmede enige wijziging, vervanging, update of latere versie daarvan.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (art. 4 lid 2 AVG).

Verwerkingsverantwoordelijke: de verantwoordelijke voor de Verwerking (art. 4 lid 7 AVG).

1.2 Begrippen die in deze Verwerkersovereenkomst met een beginhoofdletter zijn geschreven maar die niet in dit artikel zijn gedefinieerd, hebben de betekenis zoals daaraan toegekend in de Overeenkomst of de Gebruiksvoorwaarden.

Artikel 2 Algemeen

2.1 Studytube zal gedurende de uitvoering van de Overeenkomst ten behoeve van Klant Persoonsgegevens verwerken. Een overzicht van de Verwerkingen die in het kader van de Overeenkomst zullen plaatsvinden, de daarbij verwerkte Persoonsgegevens en de doeleinden van de Verwerkingen, is opgenomen in Bijsluiter A bij deze Verwerkersovereenkomst.

2.2 Studytube zal optreden als Verwerker en Klant als Verwerkingsverantwoordelijke.

2.3 Studytube garandeert dat zij ten behoeve van Klant uitsluitend Persoonsgegevens zal verwerken voor zover dit noodzakelijk is voor uitvoering van de Overeenkomst. Overige Verwerkingen zullen uitsluitend plaatsvinden op basis van schriftelijke instructies van Klant of als daartoe een wettelijke verplichting bestaat na informeren van en onder verantwoordelijkheid van Klant. Studytube zal geen Persoonsgegevens verwerken voor eigen doeleinden, behoudens voor zover zij voor de betreffende Verwerkingen zelf aangemerkt kan worden als Verwerkingsverantwoordelijke.

2.4 Studytube zal alle redelijke instructies van Klant in verband met de Verwerking van Persoonsgegevens opvolgen. Studytube stelt Klant onmiddellijk op de hoogte indien naar haar oordeel instructies in strijd zijn met toepasselijke wet- en regelgeving.
2.5 Studytube zal de Persoonsgegevens op een transparante wijze, op een rechtmatige en zorgvuldige manier en in overeenstemming met de op haar als Verwerker rustende verplichtingen verwerken.
2.6 Studytube zal een register bijhouden van alle categorieën van verwerkingsactiviteiten die zij voor Klant verricht, zulks in overeenstemming met de vereisten neergelegd in artikel 30 lid 2 en lid 3 AVG.

Artikel 3 Rechten van Betrokkenen

3.1 Studytube zal door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verlenen aan Klant om te voldoen aan haar verplichtingen op grond van de AVG, meer in het bijzonder het voldoen aan verzoeken van Betrokkenen op grond van de AVG, zoals een verzoek tot het verlenen van toegang tot hem/haar betreffende Persoonsgegevens, tot verwijdering van Persoonsgegevens, tot het rectificeren van Persoonsgegevens en/of aan te tonen dat Persoonsgegevens verwijderd of gerectificeerd zijn, de Persoonsgegevens te beperken van de Verwerking en/of tot het overdragen van de Persoonsgegevens aan een andere Verwerkingsverantwoordelijke.

Artikel 4 Beveiliging van Persoonsgegevens en Controle

4.1 Onverminderd de beveiligingsnormen die Partijen op andere wijze zijn overeengekomen, zal Studytube de verwerking van Persoonsgegevens beveiligen in overeenstemming met artikel 32 AVG, onder meer door de in Bijsluiter B uitgewerkte passende technische en organisatorische maatregelen te nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de aard van de te verwerken Persoonsgegevens, de omvang, context en doeleinden van de Verwerking, alsmede de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Betrokkenen. Deze maatregelen omvatten, waar passend, in ieder geval:
4.1.1 het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en -diensten te garanderen;
4.1.2 het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de Persoonsgegevens tijdig te herstellen;
4.1.3 een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de Verwerking.
4.2 Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging regelmatige evaluatie en verbetering van beveiligingsmaatregelen vereist. Studytube zal daarom de beveiligingsprocedure op gezette tijdstippen testen, beoordelen en evalueren, aanvullen en/of verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel. Studytube zal Bijsluiter B aanvullen of aanpassen indien dat noodzakelijk is.
4.3 Indien Klant daarom schriftelijk verzoekt, zal Studytube ten aanzien van de daarbij aangeduide (categorieën van) Persoonsgegevens bijzondere maatregelen treffen voor de beveiliging en/of de geheimhouding daarvan. Indien dit leidt tot hogere kosten voor Studytube, zal Klant deze kosten vergoeden.

Artikel 5 Meldplicht Datalekken

5.1 Zodra zich een Datalek met betrekking tot de verwerking van Persoonsgegevens voordoet of heeft voorgedaan, meldt Studytube dit zonder onredelijke vertraging nadat zij er kennis van heeft genomen aan Klant.
5.2 Studytube zal alle redelijkerwijs benodigde maatregelen nemen om (verdere) onbevoegde kennisneming, wijziging en verstrekking dan wel anderszins onrechtmatige verwerking te voorkomen of te beperken en beveiligingslekken en/of Datalekken in de toekomst zoveel mogelijk te voorkomen.
5.3 In de in lid 1 van dit artikel bedoelde melding zal Studytube alle haar bekende relevante informatie verstrekken omtrent de aard van het incident, de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpersoon waar meer informatie kan worden verkregen, de waarschijnlijke gevolgen van het incident en de maatregelen die getroffen zijn of zullen worden getroffen om het incident op te lossen dan wel de gevolgen zoveel mogelijk te beperken.
5.4 Studytube zal alle redelijke medewerking verlenen bij een eventueel onderzoek dat door Klant wordt ingesteld naar aanleiding van het incident en/of bij het formuleren van een correcte respons en bij het nemen van passende vervolgstappen ten aanzien van het incident, waaronder begrepen het informeren van de Autoriteit Persoonsgegevens en/of de Betrokkene(n).

Artikel 6 Inschakelen Subverwerkers

6.1 Studytube heeft het recht Subverwerkers in te schakelen voor activiteiten die (deels) bestaan uit het verwerken van Persoonsgegevens. De identiteit en vestigingsgegevens van op het moment van ondertekening ingeschakelde Subverwerkers zijn opgenomen in Bijsluiter A van deze Verwerkersovereenkomst. Studytube zal Klant inlichten over veranderingen inzake het toevoegen van nieuwe Subverwerkers of het vervangen van reeds ingeschakelde Subverwerkers. Klant heeft het recht daartegen bezwaar te maken.

6.2 Studytube zal de door haar ingeschakelde Subverwerkers dezelfde of strengere verplichtingen opleggen als voor haarzelf uit deze Verwerkersovereenkomst en toepasselijke wet- en regelgeving voortvloeien en ziet toe op de naleving daarvan door de Subverwerkers. De betreffende afspraken met de Subverwerkers zullen schriftelijk worden vastgelegd.

6.3 Niettegenstaande de toestemming van Klant voor het inschakelen van Subverwerkers blijft Studytube volledig aansprakelijk jegens Klant voor de gevolgen van het uitbesteden van werkzaamheden aan een Subverwerkers.

Artikel 7 Internationale doorgifte

7.1 Partijen zien er op toe dat voor zover Persoonsgegevens door Studytube buiten de Europese Economische Ruimte (EER) worden verwerkt, dit alleen plaatsvindt wanneer een passend beschermingsniveau wordt gegarandeerd. Indien Persoonsgegevens buiten de EER worden verwerkt wordt dit in Bijsluiter A aangegeven.

Artikel 8 Geheimhouding

8.1 Onverminderd enige andere contractuele geheimhoudingsverplichting die op Studytube rust, garandeert Studytube dat alle Persoonsgegevens strikt vertrouwelijk behandeld worden en dat al haar werknemers, vertegenwoordigers en/of onderaannemers die betrokken zijn bij de Verwerking van de Persoonsgegevens zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen.

Artikel 9 Bijstand aan Klant

9.1 Studytube zal Klant op verzoek alle redelijke bijstand verlenen bij het uitvoeren van een gegevensbeschermingseffectbeoordeling op grond van artikel 35 AVG en bij een eventuele voorafgaande raadpleging op grond van artikel 36 AVG. Klant zal alle kosten die Studytube maakt voor zulke bijstand volledig vergoeden.

Artikel 10 Informatievoorziening en Audits

10.1 Studytube zal Klant op verzoek alle informatie ter beschikking stellen die redelijkerwijs nodig is om nakoming van haar verplichtingen op grond van deze Verwerkersovereenkomst aan te tonen. Klant zal de in redelijkheid gemaakte kosten die Studytube voor informatieverschaffing maakt, volledig vergoeden.

10.2 Klant heeft het recht de verwerkingsactiviteiten en de genomen technische en organisatorische maatregelen te laten controleren door een onafhankelijke, gerenommeerde auditeur. Klant zal deze audits beperkt houden tot eenmaal per kalenderjaar, tenzij er een dringende noodzaak is audits vaker uit te voeren. Studytube zal medewerking verlenen aan de audits en de ingeschakelde auditeur toelaten zodat de audit daadwerkelijk uitgevoerd kan worden. De kosten van de audit worden gedragen door Klant. Klant zal de audit slechts laten uitvoeren na een voorafgaande kennisgevingsperiode aan Studytube van twee weken.

Artikel 11 Vrijwaring en Aansprakelijkheid

11.1 Klant garandeert aan Studytube dat Klant volledig gerechtigd en bevoegd is Persoonsgegevens van Gebruikers aan Studytube te verstrekken en te laten verwerken zoals overeengekomen. Klant vrijwaart Studytube volledig voor alle aanspraken van derden die op enige wijze verband houden met het niet of niet volledig naleven van deze garantie, en voor alle daarmee verband houdende schade en kosten, waaronder de volledige advocaatkosten.

11.2 Studytube is niet verantwoordelijk noch aansprakelijk voor enige Verwerkingen van Persoonsgegevens die buiten het bereik van deze Verwerkersovereenkomst vallen, waaronder de verzameling van Persoonsgegevens door Klant, Verwerkingen voor doeleinden die niet door Klant aan Studytube zijn vermeld en/of Verwerkingen door derden.

11.3 Klant vrijwaart Studytube volledig voor alle aanspraken van derden in verband met de uitvoering van deze Verwerkersovereenkomst, en voor alle daarmee verband houdende schade en kosten, waaronder de volledige advocaatkosten, tenzij Klant aantoont dat deze aanspraken een gevolg zijn van een toerekenbare tekortkoming van Studytube in de nakoming van haar verplichtingen uit deze Verwerkersovereenkomst of van nietnaleving van voorschriften die specifiek gericht zijn tot Studytube bij of krachtens de AVG.

Artikel 12 Duur en beëindiging

12.1 Deze Verwerkersovereenkomst is van toepassing zolang Studytube in verband met de Overeenkomst Persoonsgegevens verwerkt.

12.2 Na beëindiging van deze Verwerkersovereenkomst blijven de bepalingen die naar hun aard bestemd zijn om ook nadien van kracht te zijn, waaronder begrepen de bepalingen betreffende de geheimhoudingsverplichting, de aansprakelijkheid en vrijwaring en het toepasselijk recht, onverminderd van kracht.

Artikel 13 Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

13.1 Studytube bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk (i) voor uitvoering van de Overeenkomst, (ii) indien tussen Partijen een bewaartermijn is overeengekomen, niet langer dan deze termijn of (iii) om een op Studytube rustende wettelijke verplichting na te komen.

13.2 Bij beëindiging van deze Verwerkersovereenkomst, op schriftelijk verzoek van Klant of, indien van toepassing, aan het einde van de overeengekomen bewaartermijn, zal Studytube kosteloos de Persoonsgegevens, naar keuze van Klant, wissen of teruggeven aan Klant. Op schriftelijk verzoek van Klant verstrekt Studytube bewijs van het feit dat de Persoonsgegevens vernietigd of verwijderd zijn. Indien teruggave, vernietiging of verwijdering niet mogelijk is, stelt Studytube Klant daarvan onmiddellijk op de hoogte. In dat geval garandeert Studytube dat zij de Persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

13.3 Studytube maakt back-ups van het Platform en van alle Persoonsgegevens die zich daarop bevinden. Het is niet mogelijk Persoonsgegevens te verwijderen uit reeds gemaakte back-ups. Back-ups worden bewaard gedurende dertien maanden. Alle back-ups van Persoonsgegevens zullen dus uiterlijk dertien maanden na beëindiging van deze Verwerkersovereenkomst worden vernietigd of verwijderd.

13.4 Studytube heeft het recht Persoonsgegevens te anonimiseren en de geanonimiseerde data te bewaren, ook na beëindiging van deze Verwerkersovereenkomst.

13.5 Na beëindiging van deze Verwerkersovereenkomst zal Studytube alle Subverwerkers en alle derden die betrokken zijn bij het verwerken van de Persoonsgegevens op de hoogte brengen van de beëindiging van deze Verwerkersovereenkomst. De verplichtingen uit artikel 13.2 zijn van overeenkomstige toepassing op deze derden. Studytube zal waarborgen dat alle betrokken Subverwerkers en derden hieraan uitvoering zullen geven.

Artikel 14 Slotbepalingen

14.1 Wijzigingen of aanvullingen van deze Verwerkersovereenkomst worden tussen Partijen schriftelijk overeengekomen.

14.2 Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing. Alle geschillen voortvloeiend uit of samenhangend met deze Verwerkersovereenkomst worden bij uitsluiting voorgelegd aan de rechter die bevoegd is kennis te nemen van geschillen inzake de Overeenkomst.

Aldus overeengekomen en in tweevoud ondertekend,

Namens Studytube B.V.	**Namens Klant: _____**
……	……
Naam:	Naam:
Functie:	Functie:
Plaats:	Plaats:
Datum:	Datum:

Privacybijsluiter (Bijsluiter A)

I. Verwerking van Persoonsgegevens

Studytube biedt een online, geautomatiseerd systeem aan waarmee organisaties werknemers of andere medewerkers opleidingen, cursussen, trainingen en andere leervormen kunnen aanbieden, de voortgang van werknemers kunnen bijhouden en het opleidingsaanbod kunnen beheren. Om dit te doen zal Studytube Persoonsgegevens van deze werknemers of medewerkers moeten verwerken. Alle gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon kunnen worden aangemerkt als Persoonsgegevens. In deze bijsluiter wordt aangegeven welke Persoonsgegevens door Studytube worden verwerkt en waarom.

II. Rolverdeling tussen Studytube en de werkgever

Studytube biedt haar Platform aan en verricht Verwerkingen van Persoonsgegevens in opdracht van haar klanten, de organisaties die hun werknemers laten leren op het Studytube platform. Die organisaties worden hierna aangeduid als "Klant". De personen die gebruik maken van het platform worden aangeduid als "Gebruikers".

Studytube moet in het kader van de geldende privacyregelgeving worden aangemerkt als "Verwerker". De Klanten van Studytube zijn degenen die bepalen voor welk doel en met welke middelen de Persoonsgegevens van Gebruikers worden verwerkt. De Klant wordt dan ook aangemerkt als "Verwerkingsverantwoordelijke". Indien een Gebruiker vragen, klachten of verzoeken heeft betreffende de Verwerking van zijn/haar Persoonsgegevens, dient hij/zij zich dan ook te richten tot de Klant.

III. Doeleinden Verwerking van Persoonsgegevens

Bij aangaan van de Overeenkomst bepaalt Klant in overleg met Studytube voor welk hoofddoel zij de Diensten van Studytube wenst af te nemen, zoals het besteden van persoonlijk leerbudget, het verbeteren van duurzame inzetbaarheid, het delen en borgen van kennis in de organisatie, het creëren van grip op het opleidingshuis, het terugbrengen van on-boarding kosten, het aantrekken van nieuw talent of retentie van bestaande medewerkers. De inrichting van het Platform en de Diensten voor Klant en de wijze waarop Persoonsgegevens worden verwerkt is mede afhankelijk van deze keuze. Het Platform is bovendien modulair opgebouwd. Klant kan zelf kiezen welke Modules zij wenst af te nemen.

Hieronder volgt een omschrijving van de specifieke doeleinden waarvoor Studytube Persoonsgegevens ten behoeve van Klant kan verwerken.

1. Aanmaken van Gebruikersaccounts en toegang tot het Platform

Studytube verwerkt namens Klant Persoonsgegevens om Gebruikers te laten registreren, voor hen een Gebruikersaccount aan te maken en hen toegang te geven tot het Platform, waaronder identificatie, authenticatie en autorisatie. Toegang kan ook tot stand worden gebracht door middel van een technische koppeling aan systemen van Klant (single sign-on). De Gebruiker heeft de mogelijkheid Persoonsgegevens in zijn/haar Gebruikersaccount in te voeren en zijn/haar account te personaliseren.

2. Beheer van de leeromgeving door Klant

Studytube verwerkt namens Klant Persoonsgegevens om het voor de Klant mogelijk te maken de leeromgeving in te richten en te beheren. Zo kan de Klant onder andere Gebruikers per e-mail uitnodigen zich te registreren, Gebruikers aan teams toevoegen, aan Gebruikers Gebruikerslicenties voor toegang tot de Trainingsbibliotheek toekennen en Leerinterventies toewijzen aan Gebruikers. Ook kan Klant individuele opleidingsbudgetten beheren. Klant kan alle in de leeromgeving opgenomen Persoonsgegevens van Gebruikers bekijken, wijzigen en verwijderen. Ook kan Klant bepaalde categorieën Persoonsgegevens toevoegen. Dat kan ook geautomatiseerd gebeuren, door middel van een koppeling van de leeromgeving aan een HR-systeem van Klant.

3. Deelname aan Klassikale Trainingen

Studytube verwerkt namens Klant Persoonsgegevens om het mogelijk te maken dat Gebruikers een Klassikale Training kunnen aanvragen bij Klant of rechtstreeks kunnen boeken bij Externe Opleiders. Ook worden Persoonsgegevens verwerkt bij de afhandeling van Klassikale Trainingen zoals voor aanwezigheidsregistratie of het opmaken en uitreiken van certificaten.

4. Volgen van Online Trainingen

Studytube verwerkt namens Klant Persoonsgegevens zodat Gebruikers Online Trainingen kunnen volgen op het Platform, bijvoorbeeld wanneer zij vragen beantwoorden, toetsen maken, opdrachten invullen of certificaten krijgen uitgereikt.

5. Communicatie met Gebruikers

Studytube verwerkt namens Klant Persoonsgegevens om het mogelijk te maken dat er vanuit het Platform kan worden gecommuniceerd met Gebruikers. Zo worden aan Gebruikers automatische berichten verstuurd over hun

voortgang in Online Trainingen. Ook kan de Klant vanuit het Platform e-mails sturen naar Gebruikers of groepen Gebruikers.

6. Bijhouden van de voortgang van Gebruikers
Studytube verwerkt namens Klant Persoonsgegevens om het Platform zo gebruiksvriendelijk mogelijk te maken. Zo houdt Studytube de voortgang van Gebruikers bij zodat zij na inloggen direct verder kunnen met de laatst gevolgde Online Training. Ook krijgen Gebruikers inzicht in reeds gevolgde Online Trainingen.

7. Volgen en sturen van de leervoortgang door Klant
Studytube verwerkt namens Klant Persoonsgegevens om het voor de Klant mogelijk te maken de voortgang van Gebruikers te volgen en hierop bij te sturen indien nodig of gewenst. Zo kan de Klant certificaten en transacties inzien, leerinterventies toewijzen, verwijderen en wijzigen (zoals extra of andere leerlijnen, trainingen, video's of artikelen), resultaten van Online Trainingen inzien, verwijderen en downloaden en deadlines instellen. Hiertoe worden leer- en toetsresultaten opgeslagen, beoordeeld, geanalyseerd en gecombineerd, waaronder om het mogelijk te maken leerstof en toetsmateriaal af te stemmen op de specifieke leerbehoefte van de Gebruiker. Ook kan de Klant zien wanneer een Gebruiker voor het laatst actief is geweest op het Platform, wanneer de Gebruiker een Gebruikersaccount heeft aangemaakt of verwijderd en wanneer de Gebruiker heeft ingelogd.

Ook worden de door Gebruikers behaalde punten in Online Trainingen weergegeven op het Leaderboard, indien die functie door de Klant wordt ingesteld. Gebruikers kunnen deze functie in hun eigen Gebruikersaccount uitzetten zodat zij zelf niet op het Leaderboard verschijnen.

Ook kunnen rapportages worden gedownload over het aantal Gebruikers dat is uitgenodigd maar niet is geregistreerd, het totaal aantal geregistreerde Gebruikers, de meest actieve Gebruikers, het aantal minuten dat is getraind, het aantal trainingen dat is gestart en het aantal trainingen dat is afgerond en de gemiddelde review van Online Trainingen.

8. Reviews van Gebruikers
Studytube verwerkt namens Klant Persoonsgegevens teneinde het mogelijk te maken dat Gebruikers reviews geven over Online Trainingen, opleiders en het Platform en dat derden deze reviews kunnen bekijken.

9. Tonen van statistieken van Online Trainingen
Studytube verwerkt namens Klant Persoonsgegevens om statistieken voor Klant op te stellen over het gebruik van het Platform en om deze statistieken online te tonen, onder andere over de gemiddelde tijdsduur van Online Trainingen, het aantal Gebruikers in een Online Training en het aantal reviews van een Online Training.

10. Support aan Gebruikers
Studytube verwerkt namens Klant Persoonsgegevens wanneer Gebruikers aan Studytube vragen stellen door middel van de online supporttool en Studytube op verzoek van Klant Gebruikers kan ondersteunen in het gebruik van het Platform.

11. Technisch onderhoud en beheer, beveiliging en back-ups
Studytube verwerkt namens Klant Persoonsgegevens ten behoeve van beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de verwerkte Persoonsgegevens. Ook worden Persoonsgegevens namens Klant verwerkt teneinde de continuïteit en goede werking van het Platform ten behoeve van Klant te waarborgen, waaronder door het uitvoeren van onderhoud, het maken van back-ups, het aanbrengen van verbeteringen en het verlenen van ondersteuning. Onder andere wordt vastgelegd wanneer een Gebruiker inlogt en wanneer de laatste activiteit op het Platform is geweest, wanneer een Gebruiker zich registreert en voor het eerst gebruik maakt van het Platform en wanneer een Gebruiker van het Platform wordt verwijderd en niet langer van het Platform gebruik kan maken. Deze informatie is deels zichtbaar voor Klanten.

12. Verbetering product en Gebruikerservaring
Studytube verwerkt namens Klant Persoonsgegevens ten behoeve van het onderzoeken en analyseren van Gebruiksgegevens, statistieken en leer- en toetsresultaten teneinde de kwaliteit en Gebruikerservaring van het Platform te verbeteren. Voor zover deze Verwerkingen zijn gericht op verbeteringen van het Platform die niet rechtstreeks verband houden met Diensten die Studytube levert aan Klant, gebeurt dit slechts op geaggregeerd niveau en volledig anoniem (niet herleidbaar tot Gebruikers).

IV. Doorgifte aan Derden

Studytube geeft Persoonsgegevens van Gebruikers niet aan derde partijen zonder dat zij daarvoor instructie of toestemming van Klant heeft gekregen (behalve aan Subverwerkers zoals genoemd onder punt VI. hieronder). Klant geeft hierbij instructie en toestemming om Persoonsgegevens aan externe opleiders te geven in het kader van boekingen van Klassikale Trainingen door Gebruikers.

V. Overzicht per module

Hieronder wordt per Module aangegeven wat voor soort Persoonsgegevens worden verwerkt en voor welke doeleinden. Bij iedere Module is aangegeven of de Module een vast of een optioneel onderdeel is van de Diensten. Klant maakt bij het afnemen van de Diensten een keuze uit de verschillende Modules. Daarnaast kan Klant in de praktijk aanvullende Modules activeren door deze in gebruik te nemen. Een overzicht van alle afgenomen Modules zal in de jaarlijkse factuur opgenomen zijn.

Module	**Vast/ Optie**	**(Categorieën van) Persoonsgegevens**	**Doeleinde(n)**
Module 1 Bedrijfsacademy en LMS	Vast	**Vast**	
		Voornaam	1 t/m 11
		Achternaam	1 t/m 7, 9, 10, 11
		E-mailadres	1 t/m 7, 9, 10, 11
		Wachtwoord	1
		User ID	1, 6 en 10
		IP-adres	1, 6 en 11
		Datum uitnodiging verstuurd	7
		Registratiedatum	7, 11, 12
		Laatste activiteit	6, 7, 11, 12
		Inlogdatum en tijd	6, 7, 11, 12
		Datum verwijderen account	7, 11, 12
		Voortgang trainingen	4 t/m 8, 12
		Certificaten (aantal, datum, inhoud)	3 t/m 7, 12
		Datum aanvraag/transactie	3, 6, 7, 12
		Overzicht leerinterventies	6, 7, 12
		Studieresultaten leerinterventies	6, 7, 11, 12
		Optioneel	
		Aantal punten, ranking	6
		Authenticatietoken (bij single sign-on)	1
		Initialen	1 t/m 4
		Geboortedatum (bij koppeling HR)	1 t/m 4
		Functie (bij koppeling HR)	1 t/m 3
		Profielfoto (bij koppeling HR)	1
		Personeelsnummer (bij koppeling HR)	2, 3
		Identificatienummer systeem Klant (bij koppeling HR)	2
		Geboorteplaats (bij koppeling HR)	2, 3
		Geslacht (bij koppeling HR)	2, 3
		Adresgegevens (bij koppeling HR)	2, 3
		Woonplaats (bij koppeling HR)	2, 3
		Telefoonnummer (bij koppeling HR)	2, 3
		Team / organisatie info (bij koppeling HR)	2
Module 2 Online Trainingsbibliotheek	Optie	**Vast - Gelijk aan Module 1, behalve:**	
		+ Initialen	1 t/m 4
		+ Geboortedatum	1 t/m 4
		+ Antwoorden op vragen en opdrachten	4
		Optioneel - Gelijk aan Module 1, behalve:	
		+ Voorletter achternaam	8
		+ Datum review	8
		+ Review (sterren/cijfer)	8
		+ Inhoudelijke tekst review	8
Module 3 Auteurstool	Optie	**Gelijk aan Module 1**	
Module 4 Leveranciersmanagement (ABL)	Optie	**Vast - Gelijk aan Module 1, behalve:**	
		+ Functie	1 t/ 3
		+ Geboorteplaats	2, 3
		+ Geslacht	2, 3
		+ Adresgegevens	2, 3
		+ Woonplaats	2, 3
		+ Telefoonnummer	2, 3
		+ Geboortedatum	2, 3

		+ Registratie training	2
		+ Aanvraagnummer	3

VI. Subverwerkers

Studytube maakt voor het verrichten van de Diensten gebruik van de volgende Subverwerkers:

Naam	Omschrijving	Locatie verwerking
Planhat AB (Zweden)	Levert software die werknemers van Studytube door middel van diverse workflowtools helpt bij het beheren en managen van samenwerking met klanten in het behalen van hun bedrijfshoofddoelen.	EU
Hubspot, Inc.	Levert software die werknemers van Studytube via de website helpt bij het in kaart brengen van leads en marketing traffic om klanten te helpen om hun bedrijfshoofddoelen doelgericht in kaart te brengen.	US
Dropbox International Unlimited Company	Levert software waarmee werknemers van Studytube databestanden kunnen opslaan in de cloud.	EU/US
Amazon Web Services (AWS)	Hostingprovider voor de Diensten van Studytube. De servers van AWS waarvan Studytube voor haar hosting gebruik maakt zijn gevestigd in Dublin, Ierland en Frankfurt, Duitsland.	EU
Intercom, Inc.	Levert software waarmee werknemers van Studytube kunnen communiceren met klanten en Gebruikers van Studytube en eerstelijns support kunnen geven.	US
SCORM (Rustici Software)	SCORM is een technische standaard die gebruikt wordt om externe content van Klanten op het LMS van Studytube te laten draaien.	EU
Google Analytics	Levert software waarmee inzicht verkregen kan worden in het gebruik van de website en de Diensten van Studytube zodat de Gebruikerservaring en het product voor Klanten kan worden verbeterd.	EU/US

VII. Contactpersonen

Studytube
Naam en functie: Frank Vos, Legal Counsel & Privacy Officer
E-mail: legal@studytube.nl

Klant
Naam en functie: _____
E-mail: _____

Informatiebeveiligingsbeleid (Bijsluiter B)

Artikel 1 Inleiding

1.1 Definities en interpretatie

In dit informatiebeveiligingsbeleid worden de volgende begrippen als volgt gedefinieerd:
Authenticatie: Het verifiëren van de identiteit van een persoon of zaak, aan de hand van met de identiteit verbonden kenmerken, zoals een wachtwoord.
AVG: de Europese Algemene Verordening Gegevensbescherming (2016/679).
Bedrijfsmiddelen: informatie, programmatuur, fysieke bedrijfsmiddelen, diensten en immateriële zaken die door Studytube wordt gebruikt, verzameld of verwerkt.
Beheersmaatregel: technische en organisatorische voorzieningen die zijn getroffen om het beveiligingsrisico zoveel mogelijk te beperken of te beheersen, waaronder processen en richtlijnen.
Beschikbaarheid: de mate waarin gegevens, functionaliteiten of informatiesystemen op de juiste momenten beschikbaar zijn voor gebruikers en ongestoorde voortgang van de dienstverlening van Studytube gewaarborgd is.
Directie: de directie van Studytube.
Gebruikers: natuurlijke personen die op enige wijze van het systeem van Studytube gebruik maken en tot dit gebruik geautoriseerd zijn, zoals werknemers van Studytube of werknemers van klanten.
Informatiebeveiliging: Het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende beheersmaatregelen.
Informatiebeveiligingsbeleid of beveiligingsbeleid: dit Studytube informatiebeveiligingsbeleid.
Informatiebeveiligingsincident of beveiligingsincident: een geconstateerde dan wel vermoede aantasting van de vertrouwelijkheid, integriteit en/of de beschikbaarheid van het systeem of informatie alsmede situaties die het ontstaan van een (mogelijk) incident in de hand (kunnen) werken.
Informatiesystemen: de verschillende onderdelen van het systeem van Studytube waarop informatie wordt verzameld, verwerkt en/of opgeslagen.
Integriteit: de mate waarin gegevens, functionaliteiten of informatiesystemen correct juist, volledig en tijdig zijn.
ISO: Internationale Organisatie voor Standaardisatie.
Privacy Officer: de werknemer van Studytube die verantwoordelijk is voor de informatiebeveiliging en privacy.
Security Officer: de werknemer van Studytube die verantwoordelijk is voor de technische beveiliging.
Studytube: de besloten vennootschap Studytube B.V., gevestigd te Amsterdam en ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 51290901.
Systeem: het online, geautomatiseerde e-learning platform van Studytube met de verschillende informatiesystemen van Studytube.

Vertrouwelijkheid: de mate waarin de toegang tot gegevens, functionaliteiten of informatiesystemen beperkt is tot degenen die daartoe geautoriseerd zijn.
Werknemers: de werknemers van Studytube.

1.2 Algemeen

Studytube biedt een online, geautomatiseerde informatiesysteem, het platform, aan waarmee organisaties hun werknemers opleidingen, cursussen, trainingen en andere leervormen kunnen aanbieden, de voortgang van werknemers kunnen bijhouden en het opleidingsaanbod kunnen beheren. Informatie is voor Studytube het belangrijkste bedrijfsmiddel in het aanbod van het systeem en de dienstverlening aan klanten. Voor de dienstverlening aan klanten zal Studytube namens klanten informatie, waaronder persoonsgegevens, verzamelen en verwerken. De beschikbaarheid, integriteit en vertrouwelijkheid van de informatie waarborgen is voor Studytube een vereiste.

Informatiebeveiliging bestaat uit de processen en beheersmaatregelen die ingericht worden om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatiesystemen en informatie te kunnen garanderen aan onze klanten. Deze processen en beheersmaatregelen bieden bescherming tegen al dan niet opzettelijk onheil van buiten de organisatie. Aan de hand van de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid stelt Studytube risico's voor informatiebeveiliging vast, worden doelstellingen voor informatiebeveiliging bepaald en kunnen technische en organisatorische beheersmaatregelen voor informatiebeveiliging worden getroffen.

Het belang van een passende informatiebeveiliging is voor Studytube gelegen in de volgende redenen:
Privacy: De privacy (van de gebruikers) van klanten van Studytube is een vereiste van het beleid dat Studytube voert en Studytube heeft een intrinsieke motivatie om de privacy te waarborgen.
Vertrouwen: Het vertrouwen (van de gebruikers) van klanten is voor Studytube een vereiste voor het opbouwen van een succesvolle relatie. Klanten moeten erop kunnen vertrouwen dat er zorgvuldig met de gegevens van de gebruikers van hun organisatie wordt omgegaan en dat het systeem de informatie juist en volledig weer geeft.
Risicobeheersing: Wanneer informatie niet beschikbaar is, de integriteit van informatie niet wordt gewaarborgd en/of de vertrouwelijkheid van informatie wordt geschonden, kan dit schade opleveren voor de gebruiker, de klant en het imago van Studytube. Bij overtreding van wet- en regelgeving bestaat er een risico op boetes.
Concurrentie: Studytube kan zich ten opzichte van de concurrentie onderscheiden door een uitstekend informatiebeveiligingsbeleid te voeren en de privacy en het vertrouwen van klanten te waarborgen.
Efficiëntie: Informatiebeveiliging kan leiden tot de verbetering van de kwaliteit van informatie en het waarborgen van vertrouwelijkheid, zodat fouten in de uitwisseling van informatie en processen kunnen worden voorkomen.
Wetgeving: Nationale en internationale wetgeving schrijven aantoonbare passende technische en organisatorische beveiliging van informatie voor. Met dit informatiebeveiligingsbeleid voldoet Studytube aan wetgeving.

1.3 Aard en reikwijdte

Studytube heeft dit beveiligingsbeleid opgesteld om ervoor te zorgen dat informatiebeveiliging binnen Studytube wordt beheerst en dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie in het systeem gewaarborgd kan worden. Dit beveiligingsbeleid vormt een leidraad voor alle betrokkenen bij de informatiebeveiliging binnen Studytube en het kader voor de werknemers van Studytube die met informatie omgaan.

Dit beveiligingsbeleid bestaat uit uitgangspunten, principes, beheersmaatregelen, processen en richtlijnen waarmee, bij naleving daarvan, de door Studytube gestelde doelstellingen van informatiebeveiliging gehaald kunnen worden (zie artikel 2.1). Informatiebeveiliging is uiteindelijk continu in beweging en dient om die reden, evenals dit beveiligingsbeleid, periodiek aangepast te worden naarmate Studytube zich verder ontwikkelt.

Bij het opstellen van dit beveiligingsbeleid door Studytube, zijn de internationaal erkende ISO normen voor informatiebeveiliging, NEN/ISO 27001 en 27002, als uitgangspunt genomen. Studytube streeft ernaar om vóór 1 januari 2020 aantoonbaar te voldoen aan deze normen middels een geldige NEN/ISO-certificering.

1.4 Structuur

In artikel 1 wordt een algemene inleiding en de aard en reikwijdte van dit beveiligingsbeleid uiteengezet. Vervolgens wordt in artikel 2 de uitgangspunten van het beveiligingsbeleid weergegeven, waaronder de doelstellingen, verantwoordelijkheid en periodieke beoordeling. Artikel 3 geeft de classificatie van informatie weer op basis waarvan de te nemen beheersmaatregelen zijn vastgesteld en gedocumenteerd. En de artikelen 4 tot en met 15 bestaan uit twaalf artikelen met beheersmaatregelen die door Studytube zijn vastgesteld en gedocumenteerd om de informatiebeveiliging van het systeem, de informatiesystemen en de informatie zelf te kunnen waarborgen.

De ingekaderde tekstgedeelten in dit beveiligingsbeleid zijn beheersmaatregelen die een-op-een zijn overgenomen uit de NEN/ISO 27001 en 27002. De overige tekstgedeelten bevatten de uitwerkingen, in de vorm van beheersmaatregelen, processen of richtlijnen, zoals die specifiek voor Studytube zijn vastgesteld. In de meeste

gevallen zijn de gestelde maatregelen direct toegepast binnen Studytube. In andere gevallen zijn de gestelde maatregelen nader uitgewerkt in onderliggend beleid, onderliggende procedures en/of de praktische uitvoering.

Artikel 2 Uitgangspunten beveiligingsbeleid

2.1 Doelstellingen beveiligingsbeleid en informatiebeveiliging

Studytube heeft de volgende doelstellingen voor informatiebeveiliging opgesteld:
- Het beheersen van risico's op het gebied van informatiebeveiliging en het bewerkstelligen van een adequate bescherming van het systeem, de informatiesystemen en de informatie zelf.
- Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
- Het behalen van de met klanten overeengekomen contractafspraken en SLA's.
- Het voorkomen van schending van enige contractuele verplichtingen en/of gestelde beveiligingseisen.
- Het voorkomen van schending van enige wet- en regelgeving op het gebied van informatiebeveiliging.

2.2 Verantwoordelijkheid beveiligingsbeleid

ISO: Een document met informatiebeveiligingsbeleid moet door de directie worden goedgekeurd en gepubliceerd en kenbaar worden gemaakt aan alle werknemers en relevante externe partijen.

De directie stelt het beveiligingsbeleid vast, ziet toe op de implementatie en naleving van het beveiligingsbeleid, draagt het beveiligingsbeleid uit en is eindverantwoordelijke voor de informatiebeveiliging. De Security Officer en Privacy Officer verzorgen de praktische invulling van deze verantwoordelijkheid in afstemming met de directie.

Dit beveiligingsbeleid wordt vastgesteld, gepubliceerd en kenbaar gemaakt aan alle werknemers van Studytube en is daarnaast onderdeel van de contractdocumentatie met klanten van Studytube. Indien relevant en noodzakelijk voor de informatiebeveiliging wordt het beveiligingsbeleid met derden gedeeld.

2.3 Beoordeling van het beveiligingsbeleid

ISO: De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.

Het beveiligingsbeleid wordt jaarlijks, bij belangrijke wijzigingen en na (grote) informatiebeveiligingsincidenten geëvalueerd en beoordeeld om ervoor te zorgen dat het geschikt, toereikend en doeltreffend blijft. Onderliggende (beveiligings)documenten worden minimaal driejaarlijks beoordeeld of zoveel vaker als noodzakelijk.

Bij de evaluatie en beoordeling van het beveiligingsbeleid wordt gekeken naar mogelijkheden voor verbetering van het beveiligingsbeleid op basis van de werking van informatiebeveiliging, beveiligingsincidenten, terugkoppeling van belanghebbende partijen, resultaten van onafhankelijke beoordeling, veranderingen in de organisatie, wijziging van de (bedrijfs)omstandigheden, wettelijke voorwaarden en/of de technische omgeving.

Er wordt een intern verslag gemaakt van de evaluatie en beoordeling van het beveiligingsbeleid. De geïdentificeerde verbeteringen worden in een geactualiseerde versie van het beveiligingsbeleid opgenomen en ter goedkeuring voorgelegd aan de directie voordat ze worden gepubliceerd en van kracht worden.

Artikel 3 Informatiebeheer

ISO: Informatie moet worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

3.1 Kenmerken van informatie

Informatiebeheer heeft betrekking op alle in beheer zijnde gegevensverzamelingen, informatiesystemen, waaronder het systeem van Studytube, servers en netwerkcomponenten. Het object van classificatie is informatie. Wij classificeren op systeemniveau de informatie, zoals de (persoons)gegevens, die in opdracht van en namens onze klanten in het systeem worden verzameld en verwerkt voor de onze dienstverlening aan klanten.

3.2 Classificatie van informatie

Om te kunnen bepalen welke beheersmaatregelen getroffen moeten worden ten aanzien van informatiesystemen en processen, worden beveiligingsclassificaties gebruikt. Door middel van classificatie wordt het vereiste niveau van bescherming zichtbaar en wordt duidelijk welke beheersmaatregelen noodzakelijk zijn. Studytube maakt voor de classificatie van informatiebeveiliging onderscheid tussen de volgende drie kwaliteitsaspecten van informatie:

Beschikbaarheid: de mate waarin gegevens, functionaliteiten of informatiesystemen op de juiste momenten beschikbaar zijn voor gebruikers en ongestoorde voortgang van de dienstverlening van Studytube gewaarborgd is.
Integriteit: de mate waarin gegevens, functionaliteiten of informatiesystemen correct juist, volledig en tijdig zijn.
Vertrouwelijkheid: de mate waarin de toegang tot gegevens, functionaliteiten of informatiesystemen beperkt is tot degenen die daartoe geautoriseerd zijn.

De volgende tabel geeft de classificatie van informatiebeveiliging van Studytube weer ten aanzien van de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Beschikbaarheid	**Integriteit**	**Vertrouwelijkheid**
Classificatie: De beschikbaarheid van het systeem en de informatie is noodzakelijk. Algeheel verlies of niet beschikbaar zijn van het systeem of de informatie, waaronder persoonsgegevens, gedurende een werkdag brengt merkbare schade toe aan de belangen van Studytube, haar werknemers, haar klanten of haar gebruikers.	Classificatie: De integriteit van het systeem en de informatie is noodzakelijk. Informatie moet gegarandeerd correct zijn. Het gaat bijvoorbeeld om informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Bij andere informatie zijn sommige onjuistheden toelaatbaar, omdat dit eenvoudig hersteld kan worden in het systeem. Indien informatie echter niet correct is, kan Studytube, de klant of de individuele gebruiker schade lijden.	Classificatie: De informatie in het systeem van Studytube is als vertrouwelijk aan te merken. Studytube, de klant of de gebruiker kan substantiële schade lijden indien informatie, waaronder persoonsgegevens, toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die vanuit hun functie toegang moeten hebben tot deze informatie (need-to-know basis) of in zoverre het noodzakelijk is voor uitvoering van de overeenkomst met klanten.
Kenmerken: Dit betekent dat het systeem en de informatie meer dan 99% per kalendermaand beschikbaar dient te zijn, zoals voor klanten vastgelegd is in een Service Level Agreement. Daarnaast dient de Recovery Point Objective en Recovery Time Objective laag te zijn zodat gegevens niet kwijt raken en dat er weinig 'down time' is.	Kenmerken: Dit betekent dat processen binnen de diverse informatiesystemen van Studytube zoveel mogelijk foutloos dienen te verlopen. Een beperkt aantal fouten is toegestaan voor sommige vormen van informatie in het systeem naar gelang deze fouten eenvoudig in het systeem zijn te herstellen door geautoriseerde personen.	Kenmerken: Dit betekent dat informatie, waaronder persoonsgegevens, alleen toegankelijk mogen zijn voor direct betrokkenen binnen Studytube op basis van hun functie of rol of voor personen waar toegang tot de informatie noodzakelijk is voor de uitvoering van de overeenkomst met klanten.

De te nemen beheersmaatregelen door Studytube worden afgestemd op de bovenstaande classificatie en kenmerken van informatiebeveiliging, en de beveiligingsrisico's die daarmee gepaard gaan. In overeenstemming met artikel 32 van de AVG neemt Studytube passende technische en organisatorische maatregelen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de aard van de te verwerken (persoons)gegevens, de omvang, de context en doeleinden van de verwerking van (persoons)gegevens, alsmede de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.

In de navolgende artikelen van dit beveiligingsbeleid heeft Studytube de door haar genomen beheersmaatregelen, processen en richtlijnen van informatiebeveiliging vastgesteld en gedocumenteerd.

Artikel 4 Organisatie van de informatiebeveiliging

4.1 Interne organisatie

ISO: De directie behoort beveiliging binnen de organisatie te ondersteunen door richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

De directie is eindverantwoordelijke voor informatiebeveiliging en stelt het beveiligingsbeleid en de beheersmaatregelen op het gebied van informatiebeveiliging vast.

4.2 Beleid voor informatiebeveiliging in projectbeheer

ISO: Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.

Binnen Studytube wordt informatiebeveiliging meegenomen in de uitvoering van alle soorten projecten, waaronder ook de ontwikkeling of wijziging van (bestaande) informatiesystemen. Indien relevant voor projecten beoordeelt de directie projectplannen en kan zij randvoorwaarden stellen op het gebied van informatiebeveiliging.

4.3 Mobiele apparatuur en telewerken

ISO: Er moet formeel beleid zijn vastgesteld en er moeten geschikte beveiligingsmaatregelen zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

Het doel is om informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken te waarborgen. Voor de werknemers van Studytube geldt een 'bring you own device'-beleid. Hierin is onder andere vastgesteld dat de apparatuur voldoende beveiligd dient te zijn, dat er geen vertrouwelijke of gevoelige informatie op de mobiele apparatuur mag worden opgeslagen en dat er werkende virusbescherming geïnstalleerd dient te zijn. Mobiele apparatuur mag niet onbeheerd worden achtergelaten en dient anders te worden vergrendeld.

ISO: Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.

Studytube hanteert het beleid dat thuiswerken of werken op locatie zo min mogelijk plaatsvindt. Indien op afstand werken toch plaatsvindt dan hanteert de werknemer dezelfde beveiligingsmaatregelen als op kantoor.

Artikel 5 Beveiliging van personeel

5.1 Voorafgaand aan het dienstverband

ISO: De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd.

Het doel is dat toekomstige werknemers begrijpen - en dat zij geschikt zijn voor de rollen - waarvoor zij worden overwogen mede om het risico van misbruik of fraude te verminderen. Studytube versterkt het beveiligingsbewustzijn van haar werknemers door informatievoorziening. Studytube verwacht van haar werknemers onder meer dat zij (i) bijdragen aan het verwezenlijken van dit beveiligingsbeleid; (ii) de bedrijfsmiddelen behoedt tegen ongeoorloofde toegang, openbaarmaking, wijziging, vernietiging of verstoring; (iii) zorgvuldig omgaat met informatie van derden zoals klanten en leveranciers; (iv) de beveiligingsprocedures en -regels in acht neemt in de uitvoering van werkzaamheden; (v) toepasselijke wet- en regelgeving in acht neemt in de uitvoering van werkzaamheden; (vi) (potentiele) verstoringen, beveiligingsincidenten en risico's meldt conform de interne meldingsprocedure; en (vii) verantwoordelijkheid neemt voor het eigen handelen en verantwoordelijkheden ook in acht neemt bij het werken buiten de normale kantooruren en/of buiten kantoor.

ISO: Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

Alle kandidaten van Studytube worden voor een aanstelling gescreend en in het bijzonder met betrekking tot functies die als onderdeel van hun werk toegang zullen krijgen tot vertrouwelijke informatie.

ISO: Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging zijn vastgelegd.

Studytube legt haar werknemers verplichtingen op ten aanzien van geheimhouding en integriteit.

5.2 Tijdens het dienstverband

ISO: De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

Het doel is dat werknemers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, hun verantwoordelijkheid nemen en dat ze voldoende informatie hebben om het beveiligingsbeleid van Studytube in hun

dagelijkse werkzaamheden te ondersteunen. Hierdoor wordt het risico van een menselijke fout verminderd. De leidinggevenden binnen Studytube zijn verantwoordelijk voor het uitvoeren en controleren van de naleving van het beveiligingsbeleid, de procedures en regels binnen het eigen team c.q. de eigen afdeling.

ISO: Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

Alle werknemers van Studytube ontvangen passende training en regelmatige bijscholing met betrekking tot het beveiligingsbeleid en de procedures van Studytube, voor zover relevant voor hun functie.

ISO: Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

Bij overtreding van de regels voor informatiebeveiliging en/of relevante wettelijke bepalingen door een werknemer kan de directie de betreffende werknemer een sanctie opleggen conform wat hierover met betrekking tot non-actiefstelling, disciplinaire straffen en beëindiging van het dienstverband geldend is binnen Studytube.

5.3 Beëindiging of wijziging van dienstverband

ISO: De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.

Het doel van procedures bij beëindiging of wijziging van het dienstverband is om te bewerkstelligen dat werknemers ordelijk de organisatie verlaten of hun dienstverband wijzigen. Studytube hanteert duidelijke 'exit'-procedures bij beëindiging of wijziging van het dienstverband.

ISO: Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

Bij beëindiging van het dienstverband worden alle bedrijfsmiddelen van Studytube in het bezit van de betreffende werknemer geretourneerd aan Studytube, vernietigd en/of verwijderd (wat van toepassing is op de situatie).

ISO: De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

Bij beëindiging van het dienstverband wordt door Studytube alle toegangsrechten van de betreffende werknemer direct (of anders zo snel als toepasselijk) ingetrokken, zowel tot de informatiesystemen als tot het kantoor van Studytube. Bij wijziging van het dienstverband zal Studytube de relevante toegangsrechten van de betreffende werknemer direct (of anders zo snel als toepasselijk) aanpassen als dat gezien de nieuwe functie noodzakelijk is.

Artikel 6 Beleid voor toegangsbeveiliging

6.1 Bedrijfseisen ten aanzien van toegangsbeheersing

ISO: Er moet toegangsbeleid worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

Het doel van het stellen van bedrijfseisen van toegangsbeveiliging is om de toegang tot informatie te beheersen, zowel fysiek als logisch. Studytube classificeert haar informatie en informatiesystemen aan de hand van een classificatiematrix. Naarmate de classificatie hoger is, zal er een betere toegangsbeveiliging noodzakelijk zijn.

Toegang van werknemers binnen Studytube tot vertrouwelijke informatie, systeemadministratie of besturingssystemen geschiedt alleen op basis van een hoger beveiligingsniveau, is functie gebonden, wordt pas verleend na authenticatie door Studytube en is herleidbaar tot persoonsgebonden accounts door middel van logbestanden.

Studytube verleent als regel toegang tot de informatiesystemen alleen op basis van een persoonsgebonden account en op basis van een samenwerkingsovereenkomst met een klant of een individuele gebruiker. Toegangs- en managerrechten voor gebruikers van klanten worden alleen verstrekt aan personen die door vertrouwende personen bij deze klanten zijn aangemeld of volgens een andere met de klant afgesproken procedure.

ISO: Taken en verantwoordelijkheidsgebieden moeten worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Studytube past functiescheiding toe voor de diverse informatiesystemen. Toegang tot informatiesystemen is beperkt tot de gebieden die noodzakelijk zijn voor de uitvoering van de werkzaamheden van de werknemer van Studytube of voor de uitvoering van de overeenkomst met klanten. Er wordt onder andere onderscheid gemaakt tussen beheersfuncties, administratiefuncties, managersfuncties met diverse permissies en gebruikersfuncties. Daarnaast wordt door middel van toegangsrechten in de diverse informatiesystemen het risico op onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie zoveel mogelijk beperkt.

ISO: Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

Gebruikers krijgen alleen toegang het netwerk en de netwerkdiensten waarvoor zij specifiek toegang hebben gekregen via toegekende rechten. Gebruikers zullen zich eerst dienen te authentiseren voordat zij gebruik kunnen maken van de netwerkdiensten. Indien dit met klanten is overeengekomen kan Studytube gebruik maken van SAML/ADFS of IP-whitelisting zodat automatische beveiligde authenticatie van gebruikers kan plaatsvinden.

De informatiesystemen zijn extern benaderbaar via een public entry point middels beveiligd informatieverkeer. Dit geeft alleen toegang tot de functionaliteiten van de informatiesystemen en de informatie die daarop te vinden is. De besturingssystemen, applicaties en database van de informatiesystemen zijn uitsluitend intern toegankelijk via een VPN-verbinding en op basis van een persoonsgebonden instellingsaccount met een afzonderlijk token.

6.2 Beheer van toegangsrechten van gebruikers

ISO: Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd en gebruikt om toewijzing van toegangsrechten mogelijk te maken.

Het beheer van toegangsrechten van gebruikers heeft als doel om de toegang voor bevoegde gebruikers te bewerkstellingen en onbevoegde toegang tot informatiesystemen te beperken. De registratie- en uitschrijvingsprocedure wordt met de klant overeengekomen voor de toekenning van toegangsrechten aan gebruikers. Hierbij is van belang dat gebruikers vooraf geïdentificeerd en geautoriseerd worden en dat deze authenticatiegegevens overzichtelijk worden bijgehouden. Daarnaast maakt Studytube gebruik van unieke gebruikersidentificaties (ID) en controleert zij structureel of de gebruikers voldoen aan wat er contractueel met de klant is afgesproken.

ISO: Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

De gebruikerstoegangsverleningsprocedure wordt afzonderlijk per klant overeengekomen voor gebruikers en managers met diverse persmissies. Hierbij is van belang dat er wordt geregistreerd wie welke toegangsrechten heeft verkregen en dat er wordt gecontroleerd of de toegewezen persmissies geschikt zijn.

ISO: Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.

Toewijzing en wijziging van bevoorrechte toegangsrechten voor de informatiesystemen, technisch beheer of systeembeheer vindt alleen plaats na autorisatie door Studytube en wordt geregistreerd. Speciale bevoegdheden (zoals administratierechten) worden terughoudend toegekend en alleen als het nodig is voor de uitoefening van de werkzaamheden van de functie (‘need-to-use’).

ISO: Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.

Studytube heeft een wachtwoordregeling ingevoerd voor toegang tot de informatiesystemen. Voor de beveiliging van cruciale gegevens, zoals wachtwoorden, maakt Studytube gebruik van hashing via een SHA-512 encryptie.

Wanneer een gebruiker een om een (nieuw) wachtwoord verzoekt, wordt de identiteit van de gebruiker gecontroleerd aan de hand van een e-mail met instructies en een link om een wachtwoord in te vullen. Een gebruiker dient binnen korte termijn van de link gebruik te maken, anders vervalt de link. Door de versleuteling van de wachtwoorden heeft Studytube geen toegang of rechten om het wachtwoord te wijzigen namens de gebruiker, dit gaat via het systeem. Daarnaast hebben de wachtwoorden een geldigheidsduur van maximaal één jaar.

Van gebruikers van klanten wordt verwacht dat zij hun wachtwoorden nimmer onbeveiligd in leesbare vorm (digitaal) opslaan, versturen of zichtbaar nabij de werkplek tonen. Het voorgaande is voor werknemers van Studytube formeel vastgesteld. Het gebruik van een digitale wachtwoordenkluis is toegestaan, mits deze is beveiligd. Gebruikers zullen hun wachtwoord moeten veranderen als er indicaties zijn dat de wachtwoorden of een informatiesysteem gecompromitteerd is. In dat laatste geval wordt er tevens een beveiligingsincident gerapporteerd.

De toegangsrechten tot (de informatie in) de informatiesystemen van gebruikers moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd en bij wijziging moeten ze worden aangepast. Wachtwoorden van beheerders - en technische accounts worden gewijzigd bij uitdiensttreding.

ISO: Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.

De directie is verantwoordelijk voor het periodiek beoordelen van de inrichting en het gebruik van toegangsrechten tot (de informatie in) de informatiesystemen. Hierbij wordt aandacht besteed aan de rollen en de diverse functiegroepen, toegekende rechten waaronder functiescheiding, wel of niet-persoonsgebonden accounts, enz.

ISO: De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.

Voor werknemers van Studytube is formeel vastgesteld welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging van kracht blijven en gedurende welke periode. Voor klanten wordt afzonderlijk een procedure overeengekomen om de toegangsrechten van gebruikers te verwijderen of aan te passen.

6.3 Verantwoordelijkheden van gebruikers

ISO: Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.

Het doel is om onbevoegde toegang door gebruikers en beschadiging of diefstal van informatie te voorkomen. Van gebruikers van de informatiesystemen wordt dan ook verwacht dat zij: (i) hun persoonlijke accountgegevens niet delen met anderen; (ii) direct hun wachtwoord wijzigen bij het vermoeden van een lek; (iii) moeilijk te raden wachtwoorden gebruiken; (iv) wachtwoorden ten minste éénmaal per jaar wijzigen (advies is elke drie maanden); (v) wachtwoorden niet opschrijven en niet opslaan in een browser, met uitzondering van een digitale wachtwoordenkluis (mits voldoende beveiligd); (vi) wachtwoorden niet in automatische inlogprocedures gebruiken; (vii) een uniek wachtwoord gebruiken; en (viii) wachtwoorden alleen gebruiken op de correcte webpagina's.

6.4 Toegangsbeveiliging van systeem en toepassingen

ISO: Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.

Toegang tot informatie en systeemfuncties van applicaties wordt bepaald aan de hand van een autorisatiematrix. De personen zijn gekoppeld aan functies en aan deze functies zijn toegangsrechten gekoppeld.

ISO: Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.

Tijdens de inlogprocedure wordt het wachtwoord niet getoond op het scherm tijdens het ingeven. Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van 2-factor authenticatie. Bij tien foute pogingen op het wachtwoord of drie honderd requests vanaf één en hetzelfde IP-adres bij het inloggen op het systeem geldt een time-out periode van vijf minuten waarin de gebruiker niet kan inloggen.

ISO: Systemen voor wachtwoordbeheer moeten interactief zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

Bij het bepalen van de sterkte van het wachtwoord maakt Studytube gebruik van het zxcvbn-algoritme. Wachtwoorden met een zwakke sterkte worden niet geaccepteerd. Zie ook het bepaalde in artikel 6.2.

ISO: Toegang tot de programmabroncode moet worden beperkt.

Studytube beperkt de toegang tot de broncode van programmatuur zoveel als mogelijk om de broncode tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang tot de broncode.

Artikel 7 Cryptografie

7.1 Cryptografische beheersmaatregelen

ISO: Er moet beleid worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

Het doel is om de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen te beschermen. Studytube heeft passende beheersmaatregelen getroffen voor het gebruik van cryptografie (encryptie of versleuteling). Er wordt ten minste gebruik gemaakt van SSL, TLS en AES encrypties op onder meer (i) het informatieverkeer van en naar de servers van de informatiesystemen; (ii) toegang tot de beheerders- en technische omgeving; (iii) toegang tot de database van het systeem via VPN en (iv) andere situaties waar het risicoprofiel om cryptografische beheersmaatregelen vraagt. Bij cruciale gegevens, zoals wachtwoorden, maakt Studytube gebruik van hashing via SHA-512 encryptie.

ISO: Er moet sleutelbeheer zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

Voor het gebruik van cryptografische sleutels heeft Studytube sleutelbeheer ingericht. De geautoriseerde beheerder draagt onder meer zorg voor het beheer van interne (logische) sleutels, het beschermen van de systemen die gebruikt worden voor sleutels, de verwijdering van sleutels en de registratie van het sleutelbeheer.

Artikel 8 Fysieke beveiliging en beveiliging van de omgeving

8.1 Beveiligde ruimten

ISO: Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.

De fysieke- en omgevingsbeveiliging heeft als doelstelling om onbevoegde toegang tot, schade aan of verstoring van het terrein en de informatie van Studytube te voorkomen. Studytube heeft maatregelen getroffen voor de fysieke beveiliging van informatie en IT-voorzieningen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen. Alleen geautoriseerde personen hebben toegang tot niet-openbare gedeelten van het gebouw waarin Studytube is gehuisvest. De uitgifte van (magnetische) sleutels is beperkt tot geautoriseerde personen.

8.2 Beveiliging van apparatuur

ISO: Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.

Van gebruikers wordt verwacht dat zij hun apparatuur voorzien van automatische vergrendeling die na een bepaalde periode van inactiviteit in werking treedt (‘passieve vergrendeling’). Daarnaast wordt verwacht dat gebruikers hun apparatuur vergrendelen zodra zij hun werkplek voor langere duur verlaten (‘actieve vergrendeling’).

Gebruiker zijn zelf verantwoordelijk voor de apparatuur die zij onbeheerd achterlaten. Er wordt van gebruikers verwacht dat zij hun apparatuur (laptops, tablets, telefoons) zo veel mogelijk beveiligd, met schermvergrendeling en uit het zicht achterlaten. Het voorgaande is voor werknemers van Studytube formeel vastgesteld.

ISO: Er moet een ‘clear desk’-beleid voor papier en verwijderbare opslagmedia en een ‘clear screen’-beleid voor IT-voorzieningen worden ingesteld.

Studytube heeft voor haar werknemers formeel vastgesteld dat als hij of zij niet op de werkplek aanwezig is dat alle gevoelige of vertrouwelijke papieren of verwijderbare media van het bureau is verwijderd (‘clear desk’-beleid) en dat alle gevoelige of vertrouwelijke informatie van het beeldscherm wordt verwijderd en de toegang tot het beeldscherm van de werknemer wordt geweigerd (‘clear screen’-beleid). Documenten die gevoelige of vertrouwelijke informatie bevatten dienen direct van de printers te worden verwijderd na gebruik van de printer.

Artikel 9 Beveiliging bedrijfsvoering

9.1 Bedieningsprocedures en verantwoordelijkheden

ISO: Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.

De bedieningsprocedures- en verantwoordelijkheden hebben als doelstelling om een correcte en veilige bediening van de informatiesystemen te kunnen waarborgen. Studytube heeft onder meer bedieningsprocedures vastgesteld voor: (i) de aanvraag, aanmaak en verwijdering van gebruikers; (ii) het configureren van toegangsrechten; (iii) het maken en verwijderen van back-ups; (iv) het afhandelen van incidenten en calamiteiten; (v) wijzigingsbeheer; (vi) capaciteitsbeheer; (vii) systeemacceptatie en het gebruik van de ontwikkel-, test-, acceptatie en productie (OTAP)-omgevingen; (viii) het gebruik van beheer- en testtools; en (ix) logbestanden.

ISO: Veranderingen in de organisatie, bedrijfsprocessen, informatie-verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.

Studytube heeft in de procedures voor wijzigingsbeheer van informatiesystemen aandacht besteed aan (i) een impactanalyse van mogelijke gevolgen van de wijzigingen, (ii) de controle van beoogde wijzigingen door middel van tooling en (iii) vastgesteld dat wijzigingen alleen worden doorgevoerd na technische goedkeuring door de geautoriseerde beheerder die verantwoordelijk is voor beheer van de informatiesystemen ('code reviews').

Ondersteunende developers krijgen uitsluitend toegang tot onderdelen van het systeem die zij voor de uitvoering van hun werkzaamheden nodig hebben en daarnaast is formele instemming en goedkeuring nodig voor alle wijzigingen die zij willen doorvoeren in informatiesystemen ('pull requests').

9.2 Capaciteitsbeheer

ISO: Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.

Het capaciteitsbeheer heeft als doelstelling dat de dienst onder normale bedrijfsomstandigheden een overeengekomen werklast kan verwerken. Het gebruik van de dienst wordt continu gemonitord en geanalyseerd waaronder door het gebruik van tooling. Studytube ontvangt automatische notificaties als de belasting van de capaciteit boven een vastgestelde waarde uitkomt. Ongebruikelijke en/of substantiële toename van gebruik van opslag-, CPU-, geheugen- en/of netwerkcapaciteit wordt geanalyseerd en afhankelijk van het resultaat van die analyse worden passende maatregelen genomen.

Om capaciteit van het systeem te waarborgen maakt Studytube gebruik van een 'load balancer' om het binnenkomend informatieverkeer tussen de diverse servers waarvan Studytube gebruik maakt te kunnen balanceren. Bij een te hoge belasting van de capaciteit van het systeem is het via 'auto-scaling' mogelijk om nieuwe servers in de schakelen om zo de capaciteit van het systeem te verhogen.

9.3 Scheiding van ontwikkel-, test- en productieomgevingen

Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.

Studytube hanteert voor ontwikkel-, test-, acceptatiedoeleinden (OTA) aparte omgevingen, los van de productieomgeving (P). Faciliteiten voor ontwikkeling, testen, acceptatie en productie (OTAP) zijn gescheiden om onbevoegde toegang tot – of wijziging in – de informatiesystemen te voorkomen.

In de OTA worden in beginsel testaccounts gebruikt. Er wordt niet getest met productieaccounts, tenzij dit voor de test absoluut noodzakelijk is. Vertrouwelijke of geheime informatie uit de productieomgeving mag niet worden gebruikt in de OTA-omgevingen, tenzij de (persoons)gegevens onherleidbaar zijn of geanonimiseerd.

9.4 Bescherming tegen malware

ISO: Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.

De bescherming tegen malware heeft als doelstelling bedreiging van virussen om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot computersystemen zoveel mogelijk tegen te gaan en te beperken. Een groot gedeelte van de bescherming tegen virussen wordt geboden door actief 'patch management' waarbij bekende kwetsbaarheden en bedreigingen worden weggenomen. Programmatuur voor het ontdekken van kwaadaardige programmatuur is geïnstalleerd en worden regelmatig geactualiseerd.

Studytube hanteert het beleid dat alle (computer)systemen in beheer van Studytube antivirussoftware met automatisch updates zijn geïnstalleerd en dat gebruik van ongeautoriseerde programmatuur niet is toegestaan.

9.5 Back-up en recovery

ISO: Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenkomst met een overeengekomen back-upbeleid.

Back-ups hebben als doelstelling om de dienst, bij afwijkende bedrijfsomstandigheden zoals incidenten, zo snel mogelijk te herstellen. De back-ups bevatten alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd. De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienst en de interne bedrijfsvoering.

De fysieke locatie van de back-ups is op voldoende afstand van de hoofdlocatie van Studytube waardoor schade ten gevolge van een calamiteit op de hoofdlocatie onwaarschijnlijk is. De ruimte waarin de back-ups zijn opgeslagen is beschermd. De back-ups zelf zijn versleuteld aan de hand van AES-256 encryptie.

De fysiek en logische toegang tot de back-ups is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups. De back-ups en herstelprocedures worden tegelmatig getest om de betrouwbaarheid ervan vast te kunnen stellen.

9.6 Verslaglegging en monitoren

ISO: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.

De doestelling van controle, waaronder logging, is om onbevoegde gebeurtenissen of (dreigende) verstoringen te ontdekken, te kunnen analyseren en te herleiden naar gebruikers. De activiteiten van gebruikers met specifieke toegangsrechten, uitzonderingen en informatiebeveiligingsgebeurtenissen worden gelogd. Logbestanden worden ten behoeve van onderzoek en toegangscontrole bewaard, maar niet langer dan noodzakelijk en door wet- en regelgeving wordt toegestaan. In de log wordt in ieder geval de user ID, datum en tijdstip en activiteit vastgelegd.

Studytube controleert het gebruik van de informatiesystemen regelmatig. Controle van de logbestanden vindt achteraf plaats. Bij afwijkingen of ontbreken van loginformatie worden passende maatregelen genomen.

ISO: Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.

Studytube heeft een geautoriseerde beheerder aangewezen die verantwoordelijk is voor het correct functioneren en zorgvuldig beheer van het logsysteem. Logbestanden zijn voor zover mogelijk beschermd tegen mutatie en verwijdering. De logbestanden zijn verder passend beveiligd en alleen toegankelijk op een ‘need to know’ basis.

ISO: Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.

De activiteiten van systeembeheerders en -operators worden in logbestanden vastgelegd.

ISO: De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

Voor een betrouwbare analyse van de logbestanden worden systeemklokken van informatiesystemen voor zover relevant en mogelijk gesynchroniseerd met een betrouwbare centrale tijdsbron.

9.7 Beheersing van operationele software

ISO: Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.

De actualisatie van productieprogrammatuur en -toepassingen wordt uitsluitend uitgevoerd door ervaren beheerders na goedkeuring door een geautoriseerde beheerder en worden alleen geïmplementeerd na uitgebreide en succesvolle tests. Op het productiesysteem is alleen goedgekeurde uitvoerbare programmatuur aanwezig.

Voordat wijzigingen worden doorgevoerd is een terugdraaistrategie vastgesteld. Eerdere versies van de programmatuur worden bewaard voor noodgevallen en oude versies worden gearchiveerd met de noodzakelijke informatie. Daarnaast worden er logbestanden bijgehouden van de doorgevoerde wijzigingen.

9.8 Beheer van technische kwetsbaarheden

ISO: Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.

Het beheer van technische kwetsbaarheden heeft als doelstelling om te voorkomen dat technische kwetsbaarheden kunnen worden misbruikt. Studytube voert periodiek of na grote wijzigingen of uitbreiding van informatiesystemen penetratietests (“pentests”) en kwetsbaarheidscans (“vulnerability scans”) uit met gebruik van tooling.

ISO: Regels betreffend de installatie van software door gebruikers moeten vastgesteld en ingevoerd worden.

Alleen systeembeheerders hebben toegangsrechten om software te installeren voor de uitvoering van hun werkzaamheden. Gebruikers hebben geen toegangsrechten voor de installatie van software nodig.

9.9 Overwegingen betreffende audits van informatiesystemen

ISO: Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, moeten zorgvuldig worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

Bij het uitvoeren van audits worden de richtlijnen van Studytube in acht genomen zodat het risico van verstoring van de bedrijfsprocessen van Studytube zoveel mogelijk wordt beperkt. Audits worden tijdig en in overleg met Studytube besproken waarbij de reikwijdte van de audit vooraf wordt vastgesteld en daarna nageleefd.

Artikel 10 Communicatiebeveiliging

10.1 Beheer van netwerkbeveiliging

ISO: Netwerken moeten adequaat worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

Het doel is dat netwerken adequaat worden beheerd en beheerst om ze te beschermen tegen bedreigingen van buitenaf en om beveiliging te handhaven voor de systemen en toepassingen die gebruik maken van het netwerk, waaronder de transport van informatie. Netwerkbeheerders hebben maatregelen getroffen om de beveiliging van informatie in netwerken en van aangesloten diensten tegen ongeoorloofde toegang te kunnen waarborgen.

ISO: Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

Er zijn overeenkomsten gesloten met leveranciers van netwerkdiensten. De directie is verantwoordelijk voor het vaststellen van beveiligingskenmerken, niveaus van dienstverlening en de beheerseisen voor de netwerkdiensten.

ISO: Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

Informatiediensten, gebruikers en informatiesystemen zijn opgesplitst in afzonderlijke logische onderdelen met een (gelijk) functioneel gebruiksdoel. Vrijelijk informatieverkeer tussen de diverse onderdelen via het netwerk is in beginsel niet mogelijk, tenzij het verkeer noodzakelijk en goedgekeurd is.

Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of de informatiediensten, gebruikers en informatiesystemen zich nog steeds in het juiste onderdeel bevinden of dat deze verplaatst moeten worden.

Artikel 11 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

11.1 Beveiligingseisen voor informatiesystemen

ISO: In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen moeten ook eisen voor beveiligingsmaatregelen worden opgenomen.

Studytube neemt bij nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen de eisen van beveiligingsmaatregelen mee, zodat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie gewaarborgd kan worden. De beveiligingsmaatregelen zijn een afspiegeling van de waarde van de informatie voor Studytube en de mogelijke schade voor de organisatie als gevolg van het ontbreken of het falen van beveiliging. De systeemeisen voor beveiliging worden in de ontwerpfase al betrokken bij de informatiesystemen.

ISO: Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.

De servers van Studytube accepteren alleen informatieverkeer via https (SSL). Al het informatieverkeer dat wordt uitgewisseld van openbare netwerken naar de servers van Studytube is beveiligd met het https-protocol waardoor het niet mogelijk is om informatieverkeer tussen de gebruiker en Studytube te onderscheppen of te manipuleren.

ISO: Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

Voor online transacties zijn passende beveiligingsmaatregelen getroffen. Afhankelijk van de gevoeligheid of vertrouwelijkheid van de transacties wordt beheersmaatregelen genomen die in verhouding staat tot het bijpassende risiconiveau. Hierbij is het belang dat de gegevens van partijen geldig en gecontroleerd zijn, de transactie vertrouwelijk blijft, de privacy van de betrokkenen behouden blijft en dat de communicatieroute versleuteld is.

11.2 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

ISO: Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.

Informatiebeveiliging wordt bij alle ontwikkelings- en ondersteuningsprocessen van Studytube al in een vroeg stadium van de softwareontwikkeling toegepast. In plaatst van achteraf beveiliging in te bouwen in de software, heeft Studytube vastgesteld dat beveiliging al onderdeel vormt van het bedenk- en ontwikkelproces. Om tijdens het ontwikkelproces de beveiliging te kunnen waarborgen, wordt bij softwareontwikkeling structureel getest op kwetsbaarheden en het mogelijk falen van de functionaliteiten.

ISO: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.

Studytube heeft formele procedures voor wijzigingsbeheer vastgesteld om de kans op corrumperen van informatiesystemen tot een minimum te beperken. Het invoeren van nieuwe informatiesystemen en belangrijke wijzigingen in bestaande informatiesystemen volgt een formeel proces. Deze procedures omvatten onder meer: (i) waarborgen dat wijzigingen alleen worden doorgevoerd door geautoriseerde personen; (ii) goedkeuring en aanvaarding vooraf voor wijzigingen (‘code reviews’); (iii) een log van de wijzigingsaanvragen; (iv) waarborgen voor beheersmaatregelen en integriteitprocedures zodat deze niet door de wijzigingen gecompromitteerd worden; (v) het voeren van versiebeheer voor de relevant programmatuur updates en (vi) waarborgen dat de implementatie van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet worden verstoord.

ISO: Bij wijzigingen in besturingssystemen moeten bedrijfskritische toepassingen worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

Indien wijzigingen in besturingssystemen plaatsvinden worden deze getest en beoordeeld zodat beheersmaatregelen en integriteitsprocedures niet worden gecompromitteerd. Er wordt met dergelijke beoordelingen rekening gehouden in jaarlijkse planning of de development roadmap. Ook worden noodzakelijke wijzigingen in besturingssystemen tijdig aangekondigd en worden testplannen ontwikkeld voor deze beoogde wijzigingen.

ISO: Wijzigingen in programmatuurpakketten moeten worden ontmoedigd, worden beperkt tot de noodzakelijke wijzigingen, en alle wijzigingen moeten strikt worden beheerst.

Aangeleverde programmatuur wordt in de regel ongewijzigd gebruikt. Als wijzigingen in programmatuur noodzakelijk blijken te zijn, wordt er rekening gehouden met de beheersmaatregelen en integriteit van de programmatuur. De oorspronkelijke programmatuur wordt bewaard en de gewijzigde programmatuur uitvoering getest.

ISO: Principes voor het bouwen van beveiligde systemen, moeten zijn vastgesteld, beschreven, onderhouden en worden toegepast.

Studytube heeft principes vastgesteld om ervoor te zorgen dat er beveiligde informatiesystemen worden gebouwd. Bij informatiesystemen wordt structureel een afweging gemaakt tussen de noodzakelijkheid van beveiliging en de noodzakelijkheid van beschikbaarheid. Daarbij komt dat eventuele beveiligingsrisico’s worden meegewogen in de ontwikkeling. Deze principes worden periodiek beoordeeld op effectiviteit en er wordt gekeken of de principes nog up-to-date zijn gezien de huidige stand van de techniek en de potentiele beveiligingsrisico’s.

ISO: Organisatie moeten een beveiligde ontwikkelingsomgeving hebben ingericht voor de gehele levensloop van informatiesystemen.

De ontwikkelingsomgeving is een belangrijk onderdeel van de organisatie. Nieuwe informatiesystemen moeten zich ongestoord kunnen ontwikkelen, maar ongewenste beïnvloeding daarvan moet worden voorkomen. Daarbij is het ook van belang dat de deployment van de nieuwe functionaliteiten naar de productieomgeving gecontroleerd moeten plaatsvinden. De ontwikkeling van informatiesystemen vindt dan ook buiten de productieomgeving

plaats. Studytube heeft de informatiesystemen in verschillende zones geplaatst waardoor de uitwisseling van informatie niet vrijelijk kan plaatsvinden om zo de integriteit van de informatiesystemen te kunnen waarborgen.

ISO: Uitbestede ontwikkeling van programmatuur moet onder supervisie staan van en worden gecontroleerd door de organisatie.

Studytube besteedt in de regel de ontwikkeling van programmatuur niet uit. Mocht er toch sprake zijn van uitbestede ontwikkeling dan staat dit onder de supervisie en verantwoordelijkheid van de manager van het development team die toeziet op de waarborging van rechten, beschikbaarheid, kwaliteit en vertrouwelijkheid. De gemaakte afspraken hierover worden vastgelegd in een overeenkomst.

ISO: Beveiligingsfunctionaliteit moet getest worden tijdens systeemontwikkeling.

Tijdens systeemontwikkeling worden beveiligingsfunctionaliteiten structureel getest aan de hand van tooling. Van deze tests worden rapportages gedraaid en vinden 'code reviews' plaats voordat deployment plaatsvindt.

ISO: Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.

De systeemacceptatie heeft als doelstelling dat nieuwe informatiesystemen, upgrades en nieuwe versies geschikt zijn voor correct en veilig gebruik. De implementatie van nieuwe informatiesystemen, upgrades en nieuwe versies worden vooraf getoetst. Voor nieuwe informatiesystemen en grote wijzigingen vindt doorgaans een kwetsbaarheidsscan plaats door middel van tooling. Resultaten van controles of scans worden geanalyseerd en afhankelijk van die analyse worden passende maatregelen genomen voordat daadwerkelijke systeemacceptatie plaatsvindt.

ISO: Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.

In beginsel worden testaccounts en testgegevens gebruikt die operationele gegevens vervangen. In uitzonderlijke gevallen kan het noodzakelijk zijn originele gegevens te gebruiken. Er worden dan aanvullende beveiligingsmaatregelen genomen, zoals pseudonimisering, anonimisering of verwijderen van gegevens die niet nodig zijn.

11.3 Herbeoordeling technische naleving

ISO: Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

De beveiliging van de informatiesystemen en de naleving van het informatiebeveiligingsbeleid wordt periodiek gecontroleerd met behulp van een externe partij. Voorts voert Studytube met regelmaat penetratietesten ('pentests') en kwestbaarheidscans ('vulnerability scans') uit op diverse onderdelen van de informatiesystemen.

Artikel 12 Beleid voor beheersing van leveranciersdiensten

12.1 Informatiebeveiliging voor leveranciersdiensten

ISO: Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.

Studytube sluit met al haar leveranciers een overeenkomst waarin wordt overeengekomen en gedocumenteerd tot welke informatie en informatiesystemen de leverancier toegang heeft en welke eisen van informatiebeveiliging de betreffende leverancier in acht moet nemen in de uitvoering van de overeenkomst.

12.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

ISO: Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.

De directie is eindverantwoordelijke voor het besluiten welke beveiligingsclausules in de overeenkomst (algemene voorwaarden) met de leveranciers worden opgenomen. De risico's gerelateerd aan toegang van de leveranciers tot bedrijfsmiddelen van Studytube wordt hierdoor geminimaliseerd en zoveel mogelijk beperkt tot wat strikt noodzakelijk is voor de uitvoering van de overeenkomst.

12.3 Toeleveringsketen van informatie- en communicatietechnologie

ISO: Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.

Studytube heeft in haar overeenkomst met leveranciers eisen vastgelegd voor informatiebeveiliging om de risico's op beveiligingsincidenten zoveel mogelijk te beperken.

12.4 Controleren en beoordelen van leveranciers

ISO: De diensten, rapporten en registraties die door de derde partij worden geleverd, moeten regelmatig worden gecontroleerd en beoordeeld en er moeten regelmatig audits worden uitgevoerd.

Studytube controleert periodiek haar afspraken met leveranciers aan de hand van de dienstverlening, rapporten en registraties. Indien een analyse en beoordeling van die controle het rechtvaardigt, kan Studytube audits uitvoeren. Studytube kan daarnaast de afspraken met leveranciers aanpassen of de overeenkomst beëindigen.

12.5 Wijzigingen in de dienstverlening van derde partijen

ISO: Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, moeten worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

Studytube heeft in haar overeenkomsten met leveranciers vastgelegd hoe wordt omgegaan met wijzigingen in dienstverlening en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast.

Artikel 13 Informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsincidenten en zwakke plekken

ISO: Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.

Incidenten die conform de Service Level Agreement door klanten worden gemeld bij de customer support desk of via de contactpersoon bij Studytube worden als zodanig geregistreerd en voorgelegd aan de Security Officer binnen Studytube. Voor afhandeling van incidenten gelden de reactie- en hersteltijden zoals die zijn overeengekomen in de Service Level Agreement.

Informatiebeveiligingsincidenten, ofwel datalekken, worden afgehandeld conform het vastgelegde datalekkenprotocol van Studytube. Datalekken worden geregistreerd, geëvalueerd en beoordeeld. Bij afwijkingen in de informatiebeveiliging worden corrigerende maatregelen getroffen om de informatiebeveiliging te verbeteren. Melding van een datalek door Studytube wordt conform de overeengekomen verwerkersovereenkomst of de AVG gedaan aan de betrokken derde (klant, betrokkene in de zin van de AVG en/of de Autoriteit Persoonsgegevens).

ISO: Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.

Alle werknemers van Studytube dienen geconstateerde of vermoede informatiebeveiligingsincidenten zonder enige vertraging te melden bij de Privacy Officer van Studytube. Het voorgaande geldt tevens voor alle waargenomen of verdachte zwakheden van het systeem of in de dienstverlening van Studytube.

13.2 Beheer van informatiebeveiligingsincidenten en -verbeteringen

ISO: Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.

Studytube hanteert incidentenreacties met als doel het zo snel mogelijk bewerkstelligen van een beheerste situatie en het 'normale beveiligingsniveau' om vervolgens herstel te initiëren. Voor zover mogelijk en noodzakelijk wordt bewijsmateriaal van het informatiebeveiligingsincident verzameld om verdere stappen te ondernemen.

ISO: Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.

Studytube registreert beveiligingsincidenten, onder meer ten behoeve van analyse en evaluatie van de oorzaak, het verloop en de kosten van het incident. De analyse en evaluatie is met name gericht op het verbeteren van beveiligingsmaatregelen en daarmee het verkleinen van risico's. Beveiligingsincidenten worden periodiek geëvalueerd. De aanbevelingen voor verbetering van beveiligingsmaatregelen worden vastgesteld en doorgevoerd.

Artikel 14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

ISO: Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

Studytube heeft maatregelen voor bedrijfscontinuïteit getroffen waarmee de continuïteit van de informatievoorziening en de beschikbaarheid van de bedrijfsprocessen zijn gewaarborgd.

ISO: Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.

De directie heeft de taak en verantwoordelijkheid om voortdurend alert te zijn op nieuwe bedreigingen van – en risico's voor – de bedrijfscontinuïteit. Tenminste eenmaal per jaar worden de huidige maatregelen voor bedrijfscontinuïteit, en de mogelijke risico's die de continuïteit van de informatievoorziening en de bedrijfsprocessen ernstig in gevaar kunnen brengen, geanalyseerd en beoordeeld. Indien uit deze beoordeling ernstige risico's voor de bedrijfsprocessen naar voren komen worden de huidige maatregelen voor bedrijfscontinuïteit aangepast.

Artikel 15 Naleving van wettelijke en contractuele verplichtingen

15.1 Identificatie van toepasselijke wetgeving en contractuele verplichtingen

ISO: Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.

Studytube documenteert de relevante en toepasselijke wet- en regelgeving die geldt voor de dienstverlening van Studytube en die van toepassing is binnen Studytube. Studytube heeft vastgesteld wat de doeleinden zijn waarvoor de dienst van Studytube gebruikt kan worden. Studytube houdt voor zover relevant een registratie bij van de klanten die van de dienst gebruik maken, op welke manier en wie het beheer voert over deze klanten.

15.2 Privacy en bescherming van persoonsgegevens

ISO: Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Studytube bewerkstelligt de bescherming van gegevens en privacy overeenkomstig de AVG, voorschriften en contractuele bepalingen die van toepassing zijn. De informatiebeveiliging binnen Studytube is zo ingericht dat de rechten van betrokkenen die voortvloeien uit de AVG worden gerespecteerd en kunnen worden uitgeoefend.

Studytube verzamelt niet meer persoonsgegevens dan noodzakelijk voor de dienstverlening van Studytube aan klanten ('dataminimalisatie'). Voorts bewaart Studytube persoonsgegevens niet langer dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor de gegevens zijn verzameld en worden verwerkt.

Persoonsgegevens van klanten worden namens en in opdracht van de betreffende klant verwerkt op basis van een overeenkomst (waaronder een verwerkersovereenkomst). Voor alle overige verwerkingen van persoonsgegevens vormt het privacybeleid van Studytube (raad te plegen via de website van Studytube) het uitgangspunt.

15.3 Naleving van wettelijke en contractuele normen en het informatiebeveiligingsbeleid

ISO: Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

De directie is eindverantwoordelijke voor de naleving van de wettelijke en contractuele verplichtingen en de normen uit het informatiebeveiligingsbeleid. De Privacy Officer en Security Officer verzorgen de praktische invulling van deze verantwoordelijkheid in afstemming met de directie.