Informatiebeveiligingsbeleid

Versie: 1.0
Goedgekeurd door management: 02-12-2022

1 Inleiding en context

Level Up is een ICT dienstverlener die haar klanten helpt om de kwaliteit van hun interne processen te versterken. Naast het verlenen van diensten en het uitvoeren van projecten richt Level Up zich binnen de marktsegmenten Openbare Orde en Veiligheid en Onderwijs ook op de ontwikkeling van specifieke producten die ondersteunend zijn aan het primaire proces van de betrokken instellingen.

Wij bieden de volgende diensten aan klanten:

- Ontwerp, ontwikkeling, beheer en hosting van maatwerk software pakketten en standaardsoftware pakketten,
- Project- en interimmanagement,
- Business Intelligence oplossingen,
- Advies.

Het succes van Level up is mede afhankelijk van de ontwikkeling, het onderhoud en het beheer van applicaties voor onze klanten. Klanten hebben in toenemende mate de eis dat een leverancier die dergelijke diensten verleent, gecertificeerd moet zijn. In ons geval is dat NEN 7510 in verband met medische gegevens. Het is voor Level Up daarom van strategisch belang om aan de NEN 7510 normering te voldoen.

Dit beleidsdocument beschrijft de hoofdlijnen van het informatiebeveiligingsmanagement-systeem (ISMS) dat onze organisatie gebruikt. Iedereen in onze organisatie (of op sleutelposities bij leveranciers) die vertrouwelijke of gevoelige gegevens verwerkt, moet op de hoogte zijn van dit beleid en handelen in overeenstemming met het beleid.
Het volledige managementteam van ons bedrijf is betrokken geweest bij het opstellen van dit beleid en zet zich volledig in om ervoor te zorgen dat we ons aan de afspraken houden.

2 Doelstelling, scope en reikwijdte

Doelstelling

Het informatiebeveiligingsbeleid heeft als doel bij te dragen aan de kwaliteit van de informatievoorziening voor haar klanten en zichzelf en zorgdragen voor een optimale balans tussen functionaliteit, veiligheid, privacy en efficiency.

Scope

De scope van het Informatiebeveiligingsbeheersysteem (ISMS) is:
Het beveiligen van informatie in relatie tot alle informatiesystemen waar Level Up resultaatverantwoordelijk is voor onderhoud (development), beheer en hosting van deze informatiesystemen.

Toelichting op de scope: informatiesystemen die NIET worden gehost door Level Up en waar de klant dus zelf de hosting verzorgt (vaak op eigen infrastructuur van de klant), vallen NIET onder de scope van het ISMS.

Reikwijdte

Bij Level Up wordt informatieveiligheid breed geïnterpreteerd. Het gaat over alle vormen van vastgelegde informatie (dus niet alleen digitale informatie), die zij genereert en beheert.

Het beleid is locatie-onafhankelijk: het geldt ook als men op een andere locatie werkt dan in kantoorgebouwen van Level Up (zoals thuis, in de trein of op locatie bij een klant).

3 Beleidsprincipes en – uitgangspunten

Beleidsprincipes

Level Up hanteert de volgende beleidsprincipes:

1. Risico gebaseerd
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.

2. Iedereen
   Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

3. Lijnverantwoordelijkheid
   De directie is overall verantwoordelijk voor de informatiebeveiliging. Leidinggevenden dragen de verantwoordelijkheid voor de informatiebeveiliging binnen hun groep of afdeling.

4. Security by Design
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.

5. Security by Default
   Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

6. Continu proces.
   Periodiek worden beleid en maatregelen getoetst en verbeterd.

Uitgangspunten

Uit de doelstelling van informatiebeveiliging vloeien de volgende uitgangspunten voort:

- Kader
  Het beleid biedt een kader om (toekomstige) maatregelen in de informatie-beveiliging te toetsen aan de vastgestelde beveiligingsprincipes, best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden binnen het bedrijf te beleggen.

- Normen
  Level Up baseert de normen voor informatiebeveiliging op de NEN 7510 norm.

- Maatregelen
  Level Up treft maatregelen op basis van de internationaal vastgestelde NEN 7510 standaard.

- Communicatie
  Communicatie over informatiebeveiliging wordt actief bevorderd door gesprekken, bewustwordingssessies en een gedragscode.

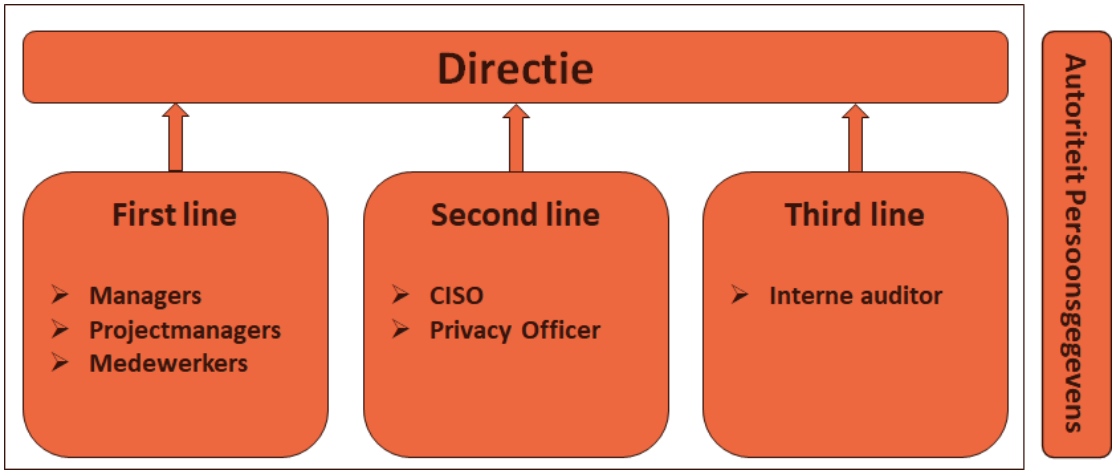
5 Governance

Organisatie van de beveiligingsfunctie

Level Up werkt vanuit een klein kernteam en een aantal vertrouwde partners die al zeer lange tijd aan Level Up zijn verbonden. Binnen het kernteam zijn de taken zodanig verdeeld dat de functiescheiding wordt gemaximaliseerd en dat het vier-ogen-principe altijd wordt toegepast in onze processen (inclusief development en deployment).

Level Up heeft twee kantoorlocaties: één in Zoetermeer en één in Rotterdam. Op dit moment zijn er geen afdelingen of bedrijfsactiviteiten specifiek buiten de scope van dit beleid verklaard.

De organisatie van de beveiligingsfunctie is opgebouwd volgens het 3-lines of defense model.



Afbeelding: 3 Lines of Defense – Level Up

Directie
De Algemeen Directeur is eindverantwoordelijk voor de informatiebeveiliging binnen Level Up en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. De portefeuillehouder van de informatiebeveiliging bij Level Up is belegd bij de ISO. De ISO is tevens verantwoordelijk voor de professionalisering van de informatiebeveiliging.

First line
Informatieveiligheid begint bij de leidinggevenden en de medewerkers. Dit houdt in dat zij eindverantwoordelijk zijn voor hun eigen informatiebeveiliging. Leidinggevenden en medewerkers dienen de door Level Up voorgeschreven beveiligingsmiddelen en informatiebeveiligingsmaatregelen te gebruiken en te volgen. Zij zijn zich bewust van relevante wet- en regelgeving en signaleren (potentiële) beveiligingsincidenten.

De 1st line is tevens verantwoordelijk voor de invoering van beheersmaatregelen en aanleveren van bewijsmateriaal dat aan de normen wordt voldaan.

Second line
De ISO rapporteert direct aan de Algemeen Directeur. De ISO draagt zorg voor de toepassing en naleving van het informatiebeveiligingsbeleid en bewaakt de compliance ten aanzien van relevante wet- en regelgeving, adviseert over informatiebeveiligingsmaatregelen en bewaakt de consistentie van de maatregelen. Daarnaast is Business Continuity Management belegd bij ISO functie alsmede de rol van Privacy Officer (PO).

De 2nd line is tevens verantwoordelijk voor het opstellen van het Informatiebeveiligingsbeleid, het opstellen van het privacy beleid, de normen en het toetsen van de naleving van de normen/beheersmaatregelen op dit gebied.

Bewustwording en training
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Bij Level Up werken we daarom voortdurend aan het verhogen van het beveiligingsbewustzijn van medewerkers met als doel om kennis van risico's te verbeteren en veilig en verantwoord gedrag aan te moedigen. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingssessies voor alle medewerkers en derden en met name operationele beheerders en ontwikkelaars.

Overleg
Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen, wordt structureel overleg gevoerd over het onderwerp informatiebeveiliging op diverse niveaus.

4 Stakeholderanalyse en maatregelen

Het managementteam van Level Up is verantwoordelijk voor het onderhouden van regelmatig contact met belanghebbenden, het begrijpen van de informatiebeveiligingseisen, het kennen van de verwachtingen van belanghebbenden en ervoor te zorgen dat het ISMS hierop is afgestemd. De resulterende informatie is gedocumenteerd in de stakeholderanalyse, die jaarlijks wordt bijgewerkt. De ISO is verantwoordelijk voor de jaarlijkse update.

In ons informatiebeveiligingsbeleid hebben wij, conform onze Verklaring van Toepasselijkheid, onder meer aandacht besteed aan beleid en maatregelen voor:

- mobiele apparatuur (A.6.2.1)
- (logische) toegangsbeveiliging (A.9.1.1);
- cryptografie (A.10.1.1);
- clear desk / clear screen (A.11.2.9);
- backup (A.12.3.1);
- informatietransport (A.13.2.1);
- beveiligd ontwikkelen (A.14.2.1);
- leveranciers (A.15.1.1).

Level Up heeft geen eigen datacentrum of servers. Alle verwerking en data worden gehost bij Microsoft Azure.