Information Security Policy

Strategische doelstelling

Het verzekeren van de informatieveiligheid is een prioriteit en een belangrijke doelstelling waarvoor het Algemeen Beheerscomité en het Directiecomité van het RIZIV zich engageren en waarvoor de Administrateur-generaal de verantwoordelijkheid opneemt. Het strategisch domein “Verbeteren van het gegevensbeheer”, opgenomen in de bestuursovereenkomst, getuigt hiervan.

Beheersysteem voor informatieveiligheid

Het beheersysteem voor informatieveiligheid (ISMS) van het RIZIV garandeert de vertrouwelijkheid, de integriteit en de beschikbaarheid van alle door de instelling verwerkte gegevens in alle bedrijfsprocessen van de kerndiensten en de ondersteunende processen van de algemene diensten. Het RIZIV engageert zich om dit beheersysteem continu te verbeteren.

Dit wordt gerealiseerd door het toepassen van risicobeheer dat op een structurele manier rekening houdt met dreigingen en opportuniteiten veroorzaakt door wijzigende technologie, wetgeving of andere omgevingsfactoren.

ISO 27001

Het RIZIV organiseert de nodige processen om het ISMS (beschreven in de ISMS Manual) in overeenstemming te brengen met de ISO 27001 standaard, de nodige controlemaatregelen te implementeren in overeenstemming met de Toepasbaarheidsverklaring en de nodige acties te organiseren voor het realiseren van onderstaande objectieven.

Objectieven Informatieveiligheid

Het RIZIV zorgt ervoor dat dit informatiebeveiligingsbeleid om de drie jaar - of bij een belangrijke wijziging - wordt herzien, rekening houdend met de minimumnormen van de Kruispuntbank van de Sociale Zekerheid en de strategie van de organisatie.

Om de informatiebeveiligingsrisico's te verminderen, zal het RIZIV-INAMI regelmatig informatiebeveiligingsrisicobeoordelingen uitvoeren en de risico's dienovereenkomstig behandelen in overeenstemming met de vastgestelde methodologie.

Om ervoor te zorgen dat alle RIZIV-medewerkers de noodzaak van informatiebeveiliging begrijpen, krijgen de medewerkers regelmatig informatiebeveiligingsbewustzijnstrainingen.

Om de vertrouwelijkheid, integriteit en beschikbaarheid van alle middelen die onder het ISMS vallen te waarborgen, zal het RIZIV-INAMI een passende reeks informatiebeveiligingscontroles documenteren en implementeren in beleid, normen en procedures, afgeleid van audits, incidentevaluaties, risicobeoordelingen, enz. die beschikbaar wordt gesteld aan en wordt meegedeeld aan alle werknemers.

Om ervoor te zorgen dat de informatiebeveiliging en de contractuele, wettelijke en reglementaire vereisten worden nageleefd, integreert het RIZIV de toepasselijke vereisten in hun strategie en dagelijkse werking.

Om de geschiktheid, geschiktheid en effectiviteit van het ISMS continu te verbeteren, zal de CISO ten minste jaarlijks managementbeoordelingen uitvoeren, rekening houdend met:

- De status van acties uit eerdere managementreviews.
- Wijzigingen die relevant zijn voor het ISMS.
- Terugkoppeling met betrekking tot non-conformiteit en correctieve acties, monitoring- en meetresultaten, auditresultaten, realisatie van de doelstellingen.
- Reacties van geïnteresseerden.
- Resultaat van risicobeoordeling en de status van risicobehandeling.
- Kansen voor continue verbetering.

Schendingen van het beveiligingsbeleid worden gemeld, onderzocht en afgehandeld via een incidentbeheerproces.