Charter voor het beveiligen van bedrijfsinformatie

Brusselsesteenweg 199, 9090 Melle • www.fluvius.be

Inhoudstafel

1 Inleiding & definitie

Om de principes van goed bestuur (*corporate governance*) na te leven heeft Fluvius System Operator het beschermen van informatie als doelstelling opgenomen.

Fluvius System Operator wenst zekerheid te bieden dat informatie op een correcte manier wordt behandeld op het vlak van vertrouwelijkheid, integriteit en beschikbaarheid (CIA[1]) door het nemen van relevante beveiligingsmaatregelen op een kostenefficiënte manier en in lijn met interne en externe wet- en regelgeving.

Om de rol van beveiliging van informatie, de organisatie en de bevoegdheden voor het beschermen van informatie formeel te definiëren, is dit Charter opgemaakt.

Door de steeds verder doorgedreven digitalisering is het noodzakelijk om informatie en systemen beleidsmatig, organisatorisch, procesmatig, technisch en operationeel te beveiligen. Het beleidsmatige wordt gerealiseerd door het opzetten van een Information Security Management System (ISMS) als governance systeem. Het organisatorische en procesmatige wordt gerealiseerd door integratie van principes voor CIA-risicobeheer.

Hierbij moet rekening gehouden worden met de steeds wijzigende interne en externe factoren, zoals wetgeving, die een invloed kunnen hebben op de opdracht van Fluvius System Operator.

De dienst Informatiebeveiliging is binnen Fluvius System Operator eindverantwoordelijk (accountable) voor het:

- Inrichten van beveiliging van informatie, onderbouwd met een beheersysteem ISMS, gebaseerd op ISO 27001
- Voldoen aan de geldende Belgische wetgeving ter zake: privacy (GDPR), NIS, Energiedecreet en andere.

2 Beveiliging van informatie

Beveiliging van informatie richt zich op alle varianten van informatie: gesproken, geschreven, gedrukt en elektronisch opgeslagen, ongeacht of het wordt gemaakt, bekeken, verwerkt, vervoerd, bewaard of vernietigd en ongeacht of de informatie komt van Fluvius zelf, zijn leveranciers of zijn klanten.

De dienst Informatiebeveiliging van Fluvius System Operator is eindverantwoordelijk voor de bescherming van informatie tegen alle relevante interne en externe bedreigingen, zowel opzettelijke als niet-opzettelijke, en zet hiervoor de nodige middelen in teneinde de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen. Door correct met informatie om

[1] CIA staat voor Confidentiality, Integrity and Availability

te gaan worden CIA-risico's beperkt tot een aanvaardbaar niveau en worden de opdrachten van Fluvius System Operator hierdoor gevrijwaard van verstoring.

Fluvius System Operator maakt gebruik van een grote diversiteit aan informatie en informatie-systemen waarbij de gevoeligheid sterk kan verschillen. Een goede informatieclassificatie is daarbij noodzakelijk om de toegang tot deze informatie en informatiesystemen risicogedreven te beheren. Fluvius System Operator wenst de vertrouwelijkheid en de integriteit van zijn informatie te kunnen waarborgen door een goede inrichting te voorzien van identiteiten, authenticatie, autorisatie en toegang.

2.1 Informatiebeveiligingsbeheersysteem

De dienst Informatiebeveiliging is eindverantwoordelijk (accountable) voor de beveiliging van informatie en zal voor goed bestuur een informatiebeveiligingsbeheerssysteem inrichten en onderhouden (Information Security Management System -ISMS), gebaseerd op ISO 27001. Dit informatiebeveiligings-beheerssysteem wordt gecertifieerd door een externe onafhankelijke firma die hiervoor geaccrediteerd is.

2.2 Basisbeveiliging van informatie

De dienst Informatiebeveiliging is verantwoordelijk voor het opstellen van richtlijnen die leiden tot technische en organisatorische maatregelen volgens de ISO 27002. Deze maatregelen vormen de basisbeveiliging van informatie en systemen. Alle afdelingen moeten deze maatregelen implementeren om hun informatie en systemen te beveiligen.

Daarnaast zijn alle afdelingen verplicht om CIA-risicobeheer uit te voeren. Hiervoor zullen zij op regelmatige basis CIA-risico´s identificeren en beoordelen. De risico-eigenaar zal in overleg met de Chief Information Security Officer (CISO) de vereiste beveiligingsmaatregelen (laten) uitvoeren om de normale werking van Fluvius System Operator blijvend te garanderen. Deze beveiligingsmaatregelen kunnen zowel beleidsmatige, organisatorische, procesmatige, technische als operationele maatregelen zijn. De dienst Informatiebeveiliging zal actief betrokken worden in geval van kritieke systemen, in geval van grote CIA-restrisico's (= CIA-risico's buiten CIA-risicoappetijt) of bij het prioriteren van de beveiligingsmaatregelen. De dienst Informatiebeveiliging neemt de overeengekomen beveiligingsmaatregelen op in een GIBP (Globaal InformatieBeveiligingsPlan) en rapporteert over de status van uitvoering.

De dienst Informatiebeveiliging legt –ingevolge de Belgische wetgeving – extra focus op het veilig beheer van persoonsgegevens, het veilig beheer van de gegevens en systemen die noodzakelijk zijn voor de uitvoeren van essentiële dienstverlening, en het volgen van andere wetgevingen zoals onder andere het Energiedecreet (databeheer).

2.3 Privacy (GDPR)

De dienst Informatiebeveiliging ziet toe op en bevordert de naleving van de Algemene Verordening Gegevensbescherming (AVG), ook wel bekend als General Data Protection Regulation (GDPR). Deze Europese verordening werd omgezet in Belgische wetgeving en heeft tot doel de persoonsgegevens van onze klanten, onze medewerkers en derde partijen op correcte manier te beschermen. Fluvius System Operator leeft de rechten van de betrokkene na, zoals het recht op correctie, uitwissing en opvraagbaarheid van de persoonsgegevens.

Door een correct beheer van de persoonsgegevens wordt vermeden dat er gegevens lekken of onrechtmatig verwerkt worden. Dit voorkomt financiële en/of imagoschade voor Fluvius System Operator of sancties door de toezichthoudende autoriteit.

2.4 NIS

Als betrouwbare partner heeft Fluvius System Operator de verantwoordelijkheid om zijn activiteiten als essentiële dienstverlener te vrijwaren. Dit omvat de naleving van de Belgische wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS-wet van 7 april 2019).

De hiervoor vernoemde “beveiliging van informatie” staat in voor een goede basisbeveiliging van informatie en -systemen, maar wordt extra versterkt om weerbaar te zijn tegen belangrijke dreigingen op digitale systemen in de essentiële dienstverlening, zowel op vlak van bescherming tegen opzettelijke bedreigingen (bv. cyberaanvallen) als op vlak van niet-opzettelijke bedreigingen (bv. menselijke fouten, technische pannes, …). Hiervoor worden er diverse activiteiten met een specifieke aanpak ingericht - in lijn met het CIA-risicoprofiel - om de essentiële en kritische infrastructuur van Fluvius te beschermen en de digitale weerbaarheid te verhogen.

3 Organisatorische invulling

Het Managementcomité staat achter het belang van het beschermen van informatie en is nadrukkelijk betrokken bij het uitdragen ervan.

De dienst Informatiebeveiliging wordt geleid door de Chief Information Security Officer (CISO), tevens Data Protection Officer (DPO), en wordt ondersteund door een team van experten.

CIA-risicobeheer voor beveiliging van informatie is een activiteit die opgevolgd maar niet uitgevoerd wordt door de dienst Informatiebeveiliging: managers uit alle directies van Fluvius System Operator laten als risico-eigenaar CIA-risicoanalyses uitvoeren volgens de richtlijnen van de dienst Informatiebeveiliging.

De CISO betrekt actief de senior managers uit de betrokken directies teneinde inspraak te bieden en een breed draagvlak te bekomen bij het bepalen van het informatiebeveiligingsbeleid zoals praktisch geïmplementeerd in het ISMS van Fluvius.

De CISO verzekert dat jaarlijks een management beoordeling gepresenteerd wordt aan het Managementcomité. De CISO kan steeds escaleren naar het Managementcomité. De CISO heeft een rapporterende lijn met een lid van het Managementcomité.

Om de informatie op een effectieve manier te beschermen is het noodzakelijk dat alle betrokkenen binnen Fluvius System Operator, vanuit hun rol en verantwoordelijkheid, bekend zijn met het Globaal InformatieBeveiligingsPlan (GIBP), dat beveiligingsmaatregelen opvolgt en zo afgestemd is op het vervullen van de opdracht en de doelstellingen.

4 Bevoegdheden

De CISO heeft van het Managementcomité het mandaat gekregen om de strategische doelstelling “beschermen van informatie” binnen Fluvius System Operator toe te passen:

1. Hiervoor moet de CISO een governance systeem inrichten en onderhouden door een op ISO27001 gebaseerd ISMS te implementeren, zodat informatie op een correcte manier wordt behandeld op het vlak van vertrouwelijkheid, integriteit en beschikbaarheid. De CISO heeft de bevoegdheid om beveiliging van informatie te versterken en te borgen door advies en voorlichting te verstrekken in de gehele organisatie.
2. De CISO heeft van het Managementcomité tevens het mandaat gekregen om als Data Protection Officer (DPO) de privacyregels van de Algemene Verordening Gegevensbescherming (AVG) binnen Fluvius System Operator toe te passen. Als DPO voert hij op een onafhankelijke wijze de opdracht uit om de privacy te bewaken bij gegevensverwerkingen, en adviseert hij de organisatie om bewust met privacy om te gaan.
3. De CISO/DPO is tevens het contactpunt tussen Fluvius System Operator en de wettelijk voorziene instanties in AVG- en NIS-wetgeving.

Alle leidinggevenden zijn verantwoordelijk voor de toepassing van de richtlijnen en procedures voor beveiliging van informatie en voor het ondersteunen van hun medewerkers bij de naleving ervan. Alle interne en externe gebruikers worden geacht om de richtlijnen en procedures voor beveiliging van informatie te volgen.

De CISO heeft de bevoegdheid om jaarlijks een aantal onderzoeken te initiëren om de geschiktheid van het managementsysteem (ISMS) te beoordelen en tijdig kwetsbaarheden binnen de organisatie te detecteren. De CISO is bevoegd om alle afwijkingen voor beveiliging van informatie in een register bij te houden. De CISO presenteert aan het Managementcomité minstens jaarlijks een management beoordeling. De CISO presenteert daarbij tevens een maturiteitsbepaling waaruit het niveau van beveiliging van informatie geconcludeerd kan worden. Bijsturing en planning van de verbeteractiviteiten worden regelmatig met het senior management besproken en jaarlijks met het Managementcomité afgestemd.

5 Onafhankelijkheid en objectiviteit

De dienst Informatiebeveiliging van Fluvius System Operator zal gevrijwaard blijven van inmenging door om het even welk element binnen de organisatie, teneinde een noodzakelijk onafhankelijke en objectieve opstelling te kunnen waarborgen.

De experten van de dienst Informatiebeveiliging zullen het hoogst mogelijk niveau van professionele objectiviteit aan de dag leggen bij het verzamelen en beoordelen van gegevens met betrekking tot hun werkzaamheden. Zij maken een evenwichtige evaluatie van alle relevante informatie en omstandigheden en worden bij vorming van hun oordeel niet beïnvloed door eigenbelang of door derden.