English below

INFORMATION SECURITY POLICY

Doel

Om de kans op een schending van de authenticiteit, integriteit, vertrouwelijkheid en beschikbaarheid van de informatie, bronnen en ict-systemen van avex te minimaliseren.

Informatiebeveiliging wordt gekarakteriseerd door het waarborgen van de vertrouwelijkheid (Bescherming van informatie tegen ongeautoriseerde toegang. Informatie is alleen toegankelijk voor degenen die daartoe bevoegd zijn.), integriteit (Zorgen voor de juistheid, volledigheid, tijdigheid en verifieerbaarheid van informatie en informatieverwerking.) en beschikbaarheid (Zorgen dat informatie en informatieverwerkingsmiddelen op het juiste moment en op de juiste plaats beschikbaar zijn voor de gebruikers.) van de informatie en de niet-weerlegbaarheid wanneer de informatie afkomstig is van een betrouwbare en geauthenticeerde bron. Bovendien zal informatiebeveiliging middelen bieden om vervalste informatie te weerleggen en het weerleggen van legitieme informatie onmogelijk te maken. Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, inclusief alle processen, organisatorische eenheden, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid past binnen het algemene beleid van AVEX en relevante wetten en regelgeving.

Meer in het algemeen is het doel van dit beleid om schade te voorkomen die kan worden veroorzaakt aan het goed functioneren van de informatiesystemen die direct door AVEX of indirect door haar dienstverleners worden beheerd.

Informatiebeveiliging kan worden bereikt door het implementeren van passende beveiligingsmaatregelen die de risico's van de organisatie minimaliseren. Om dit doel te bereiken, moeten technische maatregelen worden geïmplementeerd, evenals beleidslijnen en procedures, en moet het personeel zich bewust zijn van informatiebeveiliging en deze beleidslijnen en procedures aanpassen.

Bij het bereiken van een goede basislijn van informatiebeveiliging houden we rekening met:

- Alle wettelijke bepalingen die relevant zijn voor informatiebeveiliging, zoals privacywetgeving of wetgeving inzake computercriminaliteit.
- Ons informatiebeveiligingsbeleid is het kader voor passende personele, organisatorische en technische maatregelen om informatie te beschermen en te waarborgen, zodat de organisatie voldoet aan de relevante wetten en regelgeving. De AVEX-aanpak is risicogebaseerd. Beveiligingsmaatregelen worden genomen op basis van een inventarisatie van de kwetsbaarheid en beschermingsvereisten van de informatie, de kwetsbaarheid van de werkprocessen.

Opeenvolgende risicobeoordelingen

De waarschijnlijkheid en impact van alle huidige risico's worden opnieuw geschat. Hebben de maatregelen erin geslaagd de waarschijnlijkheid en/of impact te verminderen? Zo niet, dan moet de risicodrager beslissen hoe het resterende risico moet worden behandeld (accepteren, mitigeren, vermijden of overdragen). Nieuwe risico's kunnen worden toegevoegd op basis van recente incidenten of actuele gebeurtenissen.

Acceptatie criteria

- Alle geïdentificeerde risico's moeten worden gemitigeerd tot niveau L;
- Risico's met niveau M score 3 of hoger, moeten binnen 12 maanden worden gemitigeerd;
- Risico's met niveau H score 6 of hoger, moeten binnen 3 maanden worden gemitigeerd;
- Het management moet op de hoogte worden gebracht van alle risico's met niveau M en H.

Houd er rekening mee dat uit een Management Review blijkt dat risico's kunnen worden geaccepteerd, zelfs als ze niveau M of H hebben.

De blootstelling wordt uitgedrukt als een factor van de waarschijnlijkheid en impact. **Waarschijnlijkheid / Impact**	**Hoog** **3**	**Medium** **2**	**Laag** **1**
Hoog 3	H 9	H 6	M 3
Medium 2	H 6	M 4	L 2
Laag 1	M 3	L 2	L 1

INFORMATION SECURITY POLICY

Purpose

To minimize the chances of a breach of the authenticity, integrity, confidentiality and availability of avex's information, sources and ict systems.

Information security is characterized as ensuring the confidentiality (Protecting information from unauthorized access. Information is accessible only to those authorized to do so.), integrity (Ensuring the correctness, completeness, timeliness and verifiability of information and information processing.) and availability (Ensuring that information and information processing resources are available at the right time and in the right place for its users.) of the information and its non-repudiation when the information originates from a reliable and authenticated source. In addition, information security will provide means to refute falsified information and make refutation of legitimate information impossible. The information security policy applies to the entire organization, including all processes, organizational units, objects, information systems and data (collections). The information security policy fits within the general policy of the AVEX and relevant laws and regulations.

More generally, the objective of this policy is to prevent damage that could be caused to the proper functioning of the information systems managed by AVEX directly or by its service providers indirectly.

Information security can be achieved by implementing proper security controls that minimize the organization's risks. To achieve this goal, technical measures must be implemented as well as policies and procedures, and the personnel must be aware of information security and adapting these policies and procedures.

In achieving a good baseline of information security, we take in account:

- All legal provisions relevant to information security, such as privacy legislation or computer crime legislation.
- Our information security policy is the framework for appropriate personnel, organizational and technical measures to protect and safeguard information, so that the organization complies with relevant laws and regulations. The AVEX approach is risk-based. Security measures are taken based on an inventory of the vulnerability and protection requirements of the information, the vulnerability of the work processes.

Consecutive risk assessments

The likelihood and impact of all current risks are re-estimated. Did the measures succeed in bringing the likelihood and/or impact down? If not, the risk owner should decide how to treat the residual risk (accept, mitigate, avoid or transfer). New risks can be added based on recent incidents or current events.

Acceptance criteria

- All identified risks should be mitigated to level L;
- Risks with level M score 3 or higher, should be mitigated within 12 months;
- Risks with level H score 6 or higher, should be mitigated within 3 months;
- Management should be informed of all risks with level M and H.

Please note, that from a Management Review, risks can be accepted even when they are level M or H.

The exposure is expressed as a factor of the likelihood and impact. **Likelihood / Impact**	**High 3**	**Medium 2**	**Low 1**
High 3	H 9	H 6	M 3
Medium 2	H 6	M 4	L 2
Low 1	M 3	L 2	L 1