

Toetsingskader beveiligingsmaatregelen

1 Algemene informatiebeveiliging

1. Bij Reeleezee zijn generiek beleid en richtlijnen voor informatiebeveiliging van kracht betreffende:

- vertrouwelijkheid;
- data-integriteit;
- beschikbaarheid;
- consistentie;
- beheersbaarheid;
- audit.

2. Bij Reeleezee is een fysiek beveiligingsbeleid van kracht ter waarborging van Reeleezee's technologie, zoals bekabeling, servers, workstations en laptops.

3. Bij Reeleezee zijn fysieke en logische beveiligingsmaatregelen geïmplementeerd om de integriteit van de gegevensverwerking en data te waarborgen.

4. Rollen, verantwoordelijkheden, bevoegdheden en procedures zijn zodanig ingericht dat sprake is van een adequate functiescheiding.

5. Elk personeelslid is verplicht een beveiligingsverklaring te tekenen dat hem bindt met Reeleezee's personeelsbeveiligingsbeleid. Het personeelsbeveiligingsbeleid bevat richtlijnen omtrent:

- het gebruik van gebruikersID's en wachtwoorden;
- de inhoud van documenten;
- opslag van data;
- beveiliging van werkstations;
- installatie van software en hardware;

- verzending van vertrouwelijke informatie per email;

- fysieke beveiliging.

6. Uitsluitend geautoriseerd personeel is bevoegd de inhoud van de website van Reeleezee te veranderen. Reeleezee controleert alle veranderingen van de inhoud van de website om te waarborgen dat er geen ongeautoriseerde veranderingen worden gemaakt.

7. Reeleezee maakt gebruik van anti-virus software om de integriteit en beschikbaarheid van de toepassingen en data te waarborgen.

8. Het netwerk en de systemen van Reeleezee zijn beschermd tegen ongeautoriseerde toegang.

9. Toegang (en geweigerde toegang) tot en gebruik van het netwerk en de systemen van Reeleezee worden automatisch gemonitord. Verdachte gebeurtenissen worden onder de aandacht gebracht van Reeleezee.

10. In geval van uitbesteding zijn duidelijke afspraken gemaakt met de onderaannemer ('third-party service provider') en worden dezelfde eisen gesteld aan de onderaannemer als aan Reeleezee.

11. Naleving van afspraken met de onderaannemer wordt periodiek gecontroleerd en gerapporteerd.

12. Op de website van Reeleezee zijn de algemene verkoop- en leveringsvoorwaarden van Reeleezee gepubliceerd.

2 Vertrouwelijkheid en privacy

1. Bij Reeleezee zijn beleid en procedures van kracht om de vertrouwelijkheid van klantinformatie te waarborgen. Voorbeelden van beleid zijn:

- beleid ter attentie van gedragsregels voor het personeel;

- beleid ter attentie van de selectie van leveranciers;

- beleid ter attentie van het afgeven van garanties aan klanten (zoals bijvoorbeeld een verzekering);

- beleid ter attentie van de inzet van maatregelen en technologie.

Voorbeelden van procedures zijn:

- procedures ter attentie van de backups, inclusief bewaartermijnen;

- procedures ter attentie van de uitwerking van de personeelsgedragsregels in controlepunten;

- procedures ter attentie van informatieverstrekking aan derde partijen.

2. De Reeleezeeserver, waar de verwerking plaatsvindt, is alleen toegankelijk voor geregistreerde klanten.

3. Reeleezee's klanten die van de diensten van Reeleezee gebruikmaken mogen alleen informatie inzien of bewerken waarvan ze eigenaar zijn (informatie die betrekking heeft op henzelf of op hun eigen klanten).

4. Waar van toepassing heeft Reeleezee maatregelen getroffen aan de verwerking van persoonsgegevens teneinde te voldoen

aan de Wet bescherming persoonsgegevens (Wbp).

5. Reeleezee is een (gegevens)bewerker zoals gedefinieerd in de Wbp: "degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen".

6. Op de website van Reeleezee is een privacyverklaring opgenomen.

7. Bij uitwisseling van gevoelige (persoons) gegevens over het internet vindt versleuteling van gegevens plaats.

8. Bij Reeleezee is een personeelsbeveiligingsbeleid van kracht waarbij eisen worden gesteld aan uitgifte en ontvangst van kantooruitrusting en – benodigdheden, toegang tot werkstations en ruimten aan:

- net aangenomen personeel;

- personeel uit dienst;

- ingehuurd of gecontracteerd personeel.

9. Personeel en gecontracteerd personeel die toegang hebben tot informatie zijn verplicht een vertrouwelijkheidsverklaring te ondertekenen waarin ze verklaren geen informatie, kennis of data te onthullen welke vertrouwelijk is of welke redelijkerwijs als vertrouwelijk beschouwd kan worden.

10. Reeleezee heeft maatregelen getroffen om het beveiligingsbewustzijn van medewerkers te stimuleren (bijvoorbeeld door middel van voorlichting, documentatie of training).

11. Reeleezee controleert periodiek de naleving van de maatregelen voor vertrouwelijkheid en privacybescherming.

2. Minimaal dagelijks wordt een back-up gemaakt van Reeleezee's data en systeemconfiguratie om de mogelijkheid voor herstel te vergroten indien de primaire locatie wordt beschadigd of verwoest.

3. Back-ups worden fysiek op een andere locatie bewaard dan de primaire locatie.

4. Voor de back-ups zijn bewaartermijnen vastgesteld.

5. De hardware en bijbehorende voorzieningen zijn zodanig uitgevoerd dat bij enkelvoudige storingen de dienstverlening onverminderd wordt voortgezet.

6. Een herstelplan is aanwezig en getest om ervoor te zorgen dat, in het geval een ramp zich voordoet, de impact op de dagelijkse werkzaamheden tot een minimum wordt beperkt. De beoogde maximale uitvaltijd is drie werkdagen.

3 Beschikbaarheid

1. Reeleezee's systemen en applicaties worden tenminste elke 10 minuten automatisch op beschikbaarheid gecontroleerd (24 uur per dag, 365 dagen per jaar). Verdachte gebeurtenissen worden onder de aandacht gebracht van Reeleezee.

Meer weten?

- www.reeleezee.nl
- De Corridor 5A 3621ZA, Breukelen, Nederland
- service@reeleezee.nl
- Algemeen nummer: 0346-258080
- Helpdesk 0346-258088