Nolost Capital
a quality of life development company

Databeveiligingsbeleid

Maart 2018

Versie: 1.5.2018.03

Feeling Good, Working Better

Inhoud

Het databeveiligingsbeleid bestaat uit drie delen:

1. Vereisten medewerkers
2. Full Disk Encryptie workstation
3. Twee factor authenticatie

Op de vervolgpagina's wordt de inhoud van het beleid uit een gezet.

Deel 1: Vereisten medewerkers

1. Doelstelling

Om imagoschade te voorkomen en om een negatieve impact op onze klanten te vermijden moet Nolost Capital beperkte, vertrouwelijke of gevoelige gegevens tegen verlies beschermen. De beveiliging van relevante gegevens is een kritieke ondernemingsvoorwaarde, maar de flexibiliteit om gegevens te raadplegen en effectief te werken is dat ook.

Er wordt niet verwacht dat deze technologie doeltreffend kan omgaan met een scenario van moedwillige diefstal, of dat ze alle gegevens betrouwbaar zal detecteren. De primaire doelstelling is bewustzijn van de gebruiker en scenario's van accidenteel verlies te voorkomen. Deze regels de definiëren de eisen voor het voorkomen van datalekken, een richtpunt voor de regels en een beweegreden.

2. Omvang

1. Elke medewerker, onderaannemer of individu met toegang tot de systemen of gegevens van Nolost Capital.

2. Te beveiligen gegevens:
    - Data uit eigen medewerkersonderzoeken
    - Persoonsgegevens
    - Medewerkersgegevens van klanten
    - Bedrijfsgevoelige informatie van klanten

3. Beleid – Vereisten medewerkers

1. U moet de veiligheidsbewustzijntraining van Nolost Capital voltooien en U bekend maken met het databeveiligingsbeleid.
2. Bezoekers van Nolost Capital mogen alleen gebruik maken van het gast netwerk.
3. Toegang tot systemen dient beperkt te worden met een sterk wachtwoord, dit wachtwoord moeten uniek zijn en mag niet voor andere externe systemen of diensten gebruikt worden.
4. U dient te allen tijde bewust te zijn van het belang van goede beveiliging van gegevens.
5. Medewerkers waarvan het arbeidscontract beëindigd is moeten alle records die persoonlijke gegevens bevatten, in welk formaat ook, teruggeven.
6. U moet onmiddellijk Chris Flink op de hoogte brengen ingeval een apparaat met relevante gegevens (bijv. mobiele telefoons, laptops enz.) verloren gaat.
7. Wanneer u een systeem of proces aantreft waarvan u vermoedt dat het dit beleid of de doelstelling van informatiebeveiliging niet naleeft, moet u het management op de hoogte brengen zodat zij de juiste actie kunnen ondernemen.
8. Controleer dat de middelen die de gegevens bewaren niet onnodig in het zicht worden geplaatst, bijvoorbeeld op de achterbank van uw auto.
9. Gegevens die te verplaatsen zijn binnen Nolost Capital mogen alleen overgedragen worden via veilige transfermechanismen die door het bedrijf ter beschikking zijn gesteld (bijv. geëncrypteerde USB-sticks, bestandsdeling, e-mail enz.). Nolost Capital zal u hiertoe systemen of apparaten ter beschikking stellen. U mag geen andere mechanismen gebruiken om relevante gegevens te behandelen. Indien u vragen heeft over een transfermechanisme, of indien het niet aan uw behoeften voldoet, moet u dit opnemen met Chris Flink.
10. Alle gegevens die op een draagbaar apparaat (zoals een USB-stick, laptop) worden overgezet, moeten geëncrypteerd zijn volgens de beste praktijken in de branche en de geldende wetten en regelgeving. Indien er twijfel is over de vereisten, vraag dan advies aan Chris Flink.

Deel 2: Full Disk Encryptie werkstation

1. Doelstelling

Nolost Capital moet beperkte, vertrouwelijke of gevoelige gegevens beschermen tegen verlies om imagoschade te voorkomen en om een negatieve impact op onze klanten te vermijden. Voor een verzameling algemene regels (zoals <aanvullen naar keuze>) is ook de beveiliging van een brede scope van gegevens nodig. Dit beleid ondersteunt dat door de toegang tot gegevens gehost op <aanvullen naar keuze> apparaten te beperken.

Zoals door talrijke compliance normen en best practices uit de branche gedefinieerd, is full disk encryptie vereist om te beschermen tegen blootstelling in geval van verlies van een apparaat. Dit beleid definieert de eisen voor volledige schijfencryptie als controle- en aanverwante processen.

2. Omvang

1. Alle werkstations – desktops en laptops van Nolost Capital.
2. Alle virtuele machines van Nolost Capital.
3. Uitzonderingen: Indien er een zakelijke behoefte bestaat om dit beleid niet toe te passen (te duur, te ingewikkeld, negatieve impact op andere zakelijke noden), moet een risicoanalyse worden gevoerd die door het security management wordt goedgekeurd.

3. Beleid

1. Op alle relevante apparaten moet full disk encryptie ingeschakeld zijn.
2. Medewerkers moeten Chris Flink op de hoogte brengen indien zij vermoeden dat ze niet aan deze beleidsregels voldoen.
3. Medewerkers moeten Chris Flink op de hoogte brengen van elk apparaat dat verloren of gestolen is.
4. Het encryptiebeleid moet beheerd worden en de naleving gevalideerd door Chris Flink.
5. Een kopie van de actieve encryptiesleutel moet ter beheer aan de IT-afdeling worden aangeleverd.
6. Chris Flink heeft het recht zich toegang te verschaffen tot elk geëncrypteerd apparaat voor doeleinden van onderzoek, onderhoud of in afwezigheid van een medewerker met toegang tot primaire systeembestanden. Chris Flink en de veiligheidsbewustzijntraining zullen gebruikers van deze eis op de hoogte brengen.
7. De encryptietechnologie moet geconfigureerd worden overeenkomstig de beste praktijken om beter tegen aanvallen beschermd te worden.
8. Alle veiligheidsevents moeten gelogd en door Chris Flink geauditeerd worden om ongeoorloofde toegang tot systemen of ander kwaadaardig gebruik te identificeren.

4. Technische richtlijnen

De technische richtlijnen identificeren de eisen voor technische implementatie en zijn normaal technologiespecifiek.

Er dienen krachtige, door beste praktijken gedefinieerde cryptografische normen te worden toegepast. AES-256 is een goedgekeurde implementatie.

- Voor Mac OS X wordt XTS-AES 128 encryptie aangeraden via FileVault 2.
- Voor Windows wordt BitLocker of TrueCrypt aangeraden.

Deel 3: Twee factor authenticatie

Nolost accounts dienen beveiligd te zijn met 2 factor authenticatie (2FA). Dat betekent dat als je inlogt met je wachtwoord, je ook (via je telefoon) een tweede code in moet voeren. Dit voorkomt hacken van zwakke wachtwoorden en misbruik van gestolen wachtwoorden.

Voor instructies hoe dit het best te activeren:

- Ga naar: https://www.google.com/landing/2step/
- Klik op Button: "Getting Started" (rechtsboven)
- Volg de stappen op het scherm

De "Authenticator App" als methode is aan te raden, deze is vrij eenvoudig.

Goed om te weten is dat wanneer je in moet loggen met een applicatie die 2FA niet ondersteunt (bijvoorbeeld mail client of ophalen mail in andere account) dan moet je een app wachtwoord aanmaken, meer daarover vind je hier: https://support.google.com/accounts/answer/185833?hl=nl