Tietosuoja- ja tietoturvakuvaus

Bolt Group Oy

Ville Herva

Päivitetty 22.05.2018

Sisällysluettelo

Tämän kuvauksen soveltamisala ja tavoite

Tässä dokumentissa kuvataan Bolt Group Oy:n, sen tytäryhtiön Bolt.Works Oy:n ja mahdollisten myöhempien konserniyritysten (jäljempänä yhdessä "Bolt" tai "yhtiö") tietoturvaperiaatteet, -käytännöt ja –arkkitehtuuri.

Dokumenttia täydennetään erillisin tarkemmin järjestelmä-, prosessi- ja liiketoiminta-aluekohtaisin ohjein.

Kaikkien Boltin työntekijöiden (niin toimisto- kuin vuokra-), ulkoisten tahojen, joilla on pääsy Boltin järjestelmiin tai tietoon sekä soveltuvilta osin työnhakijoiden, asiakkaiden ja muuten Boltin palvelua hyödyntävien tulee noudattaa tämän dokumentin ohjeistusta.

Nämä ohjeet tuodaan osaksi palveluiden käyttöehtoja, käydään läpi uusien työntekijöiden perehdytyksessä sekä tuodaan tietoon ulkoisille tahoille, jotka käyttävät tai käsittelevät Boltin tietoja. Soveltuvilta osin ohjeistus velvoitetaan sopimusliitteiden kautta.

Yleiset tietoturvaperiaatteet

Suojeltava tieto ja luottamuksellisuusasteet

Bolt käsittelee tietoa sekä sähköisessä että ei-sähköisessä muodossa. Eri tyyppistä tietoa rajoittavat eri lainsäädännölliset, sopimukselliset ja muut velvoitteet. Erityisesti luottamuksellisia tietotyyppejä ovat mm. henkilötiedot, asiakkuuksiin tai muihin kumppaniyrityksiin liittyvät tiedot, muut laein tai sopimuksin luottamuksellisiksi määritetyt tiedot sekä Boltin IPR-tiedot. Näiden tietojen käsittelyssä on erityisesti noudatettava tämän dokumentin ohjeistusta. Näihin tietoihin viitataan jatkossa termillä *Boltin luottamukselliset tiedot.*

Bolt käsittelee myös muuta, luottamusasteeltaan vähäisempää tietoa, kuten Boltin työntekijöiden välinen kommunikaatio, Boltin työntekijöiden ja asiakasyritysten välinen kommunikaatio ja muut vastaavat, *jotka eivät sisällä ylemmässä kappaleessa luottamukselliseksi määrättyä tietoa.* Tällaisen tiedon käsittelyssä näitä ohjeita on noudatettava soveltuvilta osin ja milloin se ei kohtuuttomasti haittaa käsillä olevan tehtävän suorittamista.

Mikäli käsiteltävä tieto on luonteeltaan julkista tai julkiseksi tarkoitettua, sen käsittelyssä näitä ohjeita on noudatettava soveltuvilta osin ja milloin se ei kohtuuttomasti haittaa käsillä olevan tehtävän suorittamista. Vaikka julkisen tiedon joutuminen vääriin käsiin ei olekaan riski, mm. tiedon integriteetti ja oikeellisuus voi vaarantua, jos asiaankuuluvasta tietoturvasta ei huolehdita.

Mikäli tiedon luottamuksellisuuden taso ei ole selvä tämän ohjeistuksen perusteella, tietoturvavastaava päättää, miten sitä käsitellään, ja kunkin tiedonkäsittelijän on tarvittaessa kysyttävä ohjeistusta tietoturvavastaavalta ennen tiedon käsittelyyn ryhtymistä.

Tiedon tallennus ja keruu

Kaiken yhtiössä tapahtuvan henkilö- tai muuten luottamuksellisen tiedon keruulle, tallennukselle ja käsittelylle on oltava peruste, joko lakiin/asetukseen perustuva tai liiketoiminnasta johtuva. Liiketoiminnasta johtuva peruste ei voi olla ristiriidassa lakien, asetusten tai yksilön tai muiden oikeushenkilöiden oikeuksien kanssa. Tietoa tallennetaan rekistereihin (jotka voivat koostua useammasta fyysisestä järjestelmästä.) Kustakin rekisteristä tehdään seloste, jossa kuvataan tietosisältö, kunkin tietosisällön osan tallentamisen peruste, elinkaari, poistamisen prosessi sekä vastuut, roolit ja pääsyoikeudet. Poikkeuksena ovat ainoastaan tiedot, joista ei voida yksilöidä henkilöä, yritystä tai muuta tahoa, jonka suhteen tiedon käsittelyä on valvottava.

Pääsy- ja käyttöoikeudet

Kaikkeen luottamukselliseen tietoon, mukaan lukien dokumentoimat ja rekisteriin kuulumattomat tiedot, mutta erityisesti henkilö- ja yritystietoa sisältävät tietovarannot, on lähtökohtaisesti järjestettävä seuraavat ehdot täyttävä pääsynvalvonta:

- Salasanoin tai muulla vastaavalla tavalla toteutettu autentikaatio (erillinen tarkempi ohje salasanakäytännöistä, lähtökohtaisesti linjassa Vahti-ohjeiston (https://www.vahtiohje.fi/web/guest/tunnistautuminen) kanssa)
- Roolitus, jossa vain niillä (autentikoiduilla) käyttäjillä, joilla on tarve käsitellä aineistoa, on pääsy siihen. Prosessi, jossa käyttöoikeudet poistetaan, kun tarve käsittelyyn lakkaa tai henkilön rooli muuttuu
- Tarvittaessa fyysinen kulunvalvonta paikkoihin, joissa tietoa tallennetaan tai käsitellään
- Soveltuvilta osin auditointiloki siitä, kuka tietoa on käsitellyt

Kunkin roolin käyttöoikeudet on määritettävä siten, että roolilla on pääsy vain siihen aineistoon, johon pääsy on roolin mukaisen toiminnan kannalta välttämätöntä.

Tietotekniset laitteet

Kaikkien Boltin tietoteknisten laitteiden (kannettavat tietokoneet, matkapuhelimet, verkon aktiivilaitteet sekä muut vastaavat) sekä niiden käyttöjärjestelmien on toteutettava seuraavat kohdat

- Laite (ja sen käyttöjärjestelmä) valitaan siten, että ne ovat lähtökohtaisesti tietoturvallisia: niiden suunnittelussa on riittävällä tavalla huomioitu tietoturva, niillä on valmistajan puolesta uskottava tietoturvapäivitysohjelma, ja ne muuten vastaavat tietoturvaltaan käyttötarkoitusta
- Kukin laite ja sen käyttöjärjestelmä pidetään korkeintaan viikon viiveellä ajan tasalla tietoturvapäivitysten suhteen
- Soveltuvilta osin laitteeseen asennetaan virustorjunta tai palomuuri, jollei laitteen tietoturva muuten ole riittävällä tasolla tai laite luonteeltaan sellainen, ettei jompaakumpaa tarvita
- Laitteen asennus ja konfigurointi tehdään niin, että tietoturvariskit minimoidaan (mm. ajossa olevat palvelut minimoidaan)
- Laite sijoitetaan verkkoinfrastruktuuriin niin, että sen altistuminen verkkohyökkäyksiin on pienin mahdollinen käyttötarkoitusta rajoittamatta

Laitevalinnoista ja laitteiden valitsemisesta ja päivittämisestä vastaa it-osasto.

Tietojärjestelmät ja palvelut

Kaikkien Boltin tietoteknisten järjestelmien ja palveluiden (myös ulkopuolisten palveluntarjoajien SAAS-mallilla tarjoamat) on toteutettava seuraavat kohdat

- Järjestelmä tai palvelu valitaan siten, että se on lähtökohtaisesti tietoturvallinen: sen suunnittelussa on riittävällä tavalla huomioitu tietoturva, sillä on toimittajan puolesta uskottava tietoturvapäivitysohjelma, ja se muuten vastaa tietoturvaltaan käyttötarkoitustaan
- Kukin järjestelmä tai palvelu, sekä sen alusta (laitteisto, käyttöjärjestelmä, tukijärjestelmät) pidetään korkeintaan viikon viiveellä ajan tasalla tietoturvapäivitysten suhteen
- Soveltuvilta osin järjestelmän tai palvelun palvelualusta on suojattu palomuurilla tai intrusion detection -järjestelmällä, jollei alustan tietoturva muutoin ole riittävällä tasolla
- Järjestelmän ja alustan asennus ja konfigurointi tehdään niin, että tietoturvariskit minimoidaan
- Palvelu on sijoitettu verkkoinfrastruktuuriin niin, että sen altistuminen verkkohyökkäyksiin on pienin mahdollinen käyttötarkoitusta rajoittamatta

Järjestelmien ja palveluiden valitsemisesta ja päivittämisestä vastaa it-osasto sekä ulkoiset palveluntarjoajat sopimuksin velvoitettuina.

Henkilöturvallisuus

Soveltuvilta osin tietoihin tai palveluin käsiksi pääsevien henkilöiden henkilöllisyys ja rooli tarkistetaan.

Tarvittaessa toteutetaan turvaselvitys henkilöstä, jolla on tarve antaa pääsy luottamukselliseen aineistoon.

Ulkoiset tahot

Mikäli ulkoisen tahon on perusteltua käsitellä Boltin hallinnoimia tai omistamia tietoja, jotka ovat tämän dokumentin mukaisesti suojeltavia, kyseinen ulkoinen taho velvoitetaan sopimuksella noudattamaan näitä periaatteita. Sopimuksellisen velvoitteen on koskettava kaikkia ulkoisen tahon edustajia, joilla on päästy tietoon. Sopimuksellisen velvoitteen tulee kieltää ulkoista tahoa edelleen luovuttamasta tietoa tai muuten päästämään mitään kolmatta osapuolta käsittelemään tietoa ilman Boltin kirjallista lupaa ja erillistä sopimusta. Sopimuksellisen velvoitteen on täytettävä Euroopan parlamentin ja neuvoston asetuksen luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU:n tietosuoja-asetus 2016/679) vaatimukset henkilörekisterin käsittelijän sopimusvelvoitteesta.

Cyber- ja muut uhat

Tietojen luottamuksellisuuteen ja integriteettiin kohdistuvia cyber- ja muita uhkia ovat mm. tietoturvapoikkeamat sekä -hyökkäykset, yritysvakoilu, virukset, tietojärjestelmien heikkoudet sekä viat, fyysiset uhat (kuten tulipalo ja luonnon ilmiöt), sabotaasi ja terrorismi. Bolt varautuu näihin, mm. noudattamalla ammattimaista tietoturvaa (tämän dokumentin mukaisesti), varmistamalla tietoa

ammattimaisesti huomioiden fyysisen luotettavuuden, redundanssin, varmuuskopiot ja saavutettavuuden sekä fyysisin varotoimin (paloturvallisuus, kulunvalvonta.) Viime kädessä haittoja mitigoidaan vakuutuksin.

Poikkeamista, jotka ovat vaarantaneet luottamuksellisten tietojen integriteetin tai luottamuksellisuuden raportoidaan (sovellettavaa lainsäädäntöä noudattaen) viranomaisille, ja tahoille joihin viittaava tieto on vaarantunut (esim. henkilötietojen tapauksissa.)

Tietoturvaa ohjaavat tekijät

Yhtiön tietoturvatoiminnassa noudatetaan johtoryhmän ohjeistuksia tai tätä kuvausta. Tämän lisäksi toimintaa ohjaavat seuraavat tietoturvaan liittyvät lait:

- Laki viranomaisen toiminnan julkisuudesta (julkisuuslaki 1999/621)
- Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU:n tietosuoja-asetus 2016/679)
- Henkilötietolaki (1999/523)
- Laki yksityisyyden suojasta työelämässä (2004/759)
- Tietoyhteiskuntakaari (2014/917)
- Turvallisuusselvityslaki (2014/726)
- Rikoslaki (1889/39)

Tietosuojan osalta noudatetaan EU:n tietosuoja-asetusta sekä sitä tarkentavaa kansallista lainsäädäntöä. Yhtiössä on nimetty, muista tehtävistä riippumaton tietosuojavastaava.

Tietoturvan kehittämistä ohjaa vaatimustenmukaisuuden lisäksi tieto-omaisuuteen, tietojärjestelmiin ja toimintaympäristöön kohdistuvien riskien tunnistaminen ja niiden vaikutusten arviointi.

Vastuut ja tietoturvan kehittämisprosessi

Bolt-konsernin tietoturvasta vastaa Bolt Group Oy:n toimitusjohtaja tietoturvavastaavan avustamana. Tietoturvavastaava myös vastaa tietoturvallisuuden toteutumisesta ja johtaa tietoturvaan liittyvää operatiivista toimintaa.

Tietosuojasta vastaa rekisterinpitäjä. Tietosuojavastaava seuraa ja valvoo, että tietosuoja-asetusta sekä muita tietosuojalainsäännöksiä ja rekisterinpitäjän toimintamenettelyjä noudatetaan. Tietoturvan- ja suojan toimeenpanoa ohjaavat tietoturvapäällikkö ja tietosuojavastaava.

Tietoturvan toteuttamisesta teknisissä järjestelmissä (tekninen tietoturva) vastaa osalta IT-osasto. IT-osastolla tulee olla riittävä asiantuntemus teknisten ratkaisujen määrittelyyn ja toteuttamiseen sekä tietoverkkojen ja –järjestelmien tietoturvavalvontaan. Yksiköiden omien palveluiden osalta teknisten järjestelmien tietoturvan toteutumisesta ja valvonnasta vastaa järjestelmän omistaja. Tietoturvavastaava koordinoi IT-palveluiden ja yksiköiden teknisen tietoturvan toteuttamista.

Esimiesten tehtävä on huolehtia, että heidän henkilöstönsä tuntee tietoturvaperiaatteet ja -vastuut ja saa tarvittavan koulutuksen.

Jokainen toimistohenkilökunnan jäsen ja soveltuvilta osin vuokratyöntekijä sekä Boltin tarjoamiin palveluihin käyttöoikeuden saanut käyttäjä on velvollinen noudattamaan annettuja ohjeita. Jokainen vastaa omalla toiminnallaan tietoturvan toteutumisesta ja edistää hyvän tietoturvakulttuurin kehittymistä.

Tietoturvaperiaatteiden ja –ohjeiden noudattaminen

Jokaisen Boltiin työsopimus-, asiakas- tai työnhakusuhteessa oleva henkilö on velvollinen noudattamaan tässä asiakirjassa määriteltyjä periaatteita ja niitä täsmentäviä ohjeita, muita Boltin antamia tietoturvaohjeita sekä tietojärjestelmien, -verkkojen, -koneiden ja -välineiden käyttösääntöjä. Politiikoiden, periaatteiden tai ohjeiden laiminlyöminen tai niiden vastaisesti toimiminen katsotaan tietoturvarikkeeksi.

Tietoturvaperiaatteiden ja ohjeiden tarkoituksellinen laiminlyönti voi johtaa seuraamuksiin. Henkilökunnan seuraamukset tietoturvarikkeen johdosta voivat olla rikkeen vakavuudesta riippuen

1. ohjaava puhuttelu
2. suullinen huomautus
3. kirjallinen varoitus
4. irtisanominen
5. työsuhteen purkaminen

Ohjaavan puhuttelun pitää tietoturvavastaava. Muiden seuraamusten osalta toimivalta niiden päättämisestä määräytyy työsopimuslain perusteella.

Muut Bolt-palveluiden käyttäjän seuraamukset tietoturvarikkeen johdosta voivat olla

1. Ohjeistus
2. Suullinen huomautus
3. Kirjallinen varoitus
4. Palvelun tai tietoon käsiksi pääsyn estäminen

Ohjeistuksen antaa tietoturvavastaava. Muiden seuraamusten osalta toimivalta seuraamusten suhteen noudatetaan tehtyjä sopimuksia.

Tietojärjestelmien käyttösäännöissä kuvataan tarvittaessa esimerkein rikkeitä, niiden vakavuutta ja seuraamuksia.

Mikäli rikkeeseen liittyy rikosepäily, päättää toimitusjohtaja tutkintapyynnön tekemisestä poliisille. Rikosepäilyn tapauksessa Bolt voi sulkea käyttöoikeudet määräajaksi. Käyttöoikeudet voidaan sulkea myös, mikäli yhtiön tietoturva merkittävästi vaarantuu käyttäjän toiminnan takia.

Tietoturvapolitiikan ja –periaatteiden hyväksyntä ja ylläpito

Tietoturvapolitiikan ja -periaatteiden valmistelusta ja ylläpidosta vastaa tietoturvavastaava.

Tietoturvakuvauksen ja –periaatteet katselmoi ja hyväksyy konsernin johtoryhmä vähintään vuoden välein.

Sopimuskumppaneita tiedotetaan tarpeen mukaan.

Roolit ja pääsynvalvonta

Kullekin luottamuksellisen tiedon tietorekisterille on rekisteriselosteen yhteydessä kuvattava roolit ja niitä vastaavat pääsyoikeudet. Kyseiset pääsyoikeudet on toteutettava kaikissa teknisissä järjestelmissä, joissa rekisterin tietoa säilytetään.

Tarvittaessa rekisterin käyttöä valvotaan myös lokitiedostoin, joista voidaan todentaa, kuka tietoa on käsitellyt ja milloin.

Haavoittuvuudet, paikkaukset ja ohjelmistoversioiden päivityskäytännöt

Tietojärjestelmien (fyysisen laitteiston, tietoliikennejärjestelmien, käyttöjärjestelmien, palvelinohjelmistojen ja sovellusohjelmistojen) tietoturvapäivitykset asennetaan pääsääntöisesti välittömästi, kun se on käyttöä kohtuuttomasti haittaamatta mahdollista ja kun henkilöstö voi sen mm. työaikojen puitteissa tehdä. Poikkeuksena tilanteet, joissa voidaan aukottomasti todeta, että kyseinen tietoturvahaavoittuvuus ole Boltin käyttötapauksessa relevantti. Tällaisesta päätöksestä vastaa viimekädessä tietoturvavastaava. Bolt myötävaikuttaa siihen, että kaikki järjestelmätoimittajat ja kumppanit, joiden palvelun kautta Boltin luottamukselliset tiedot voivat joutua vaaraan, noudattavat samaa periaatetta, ja keskeyttää tarvittaessa sellaisen palvelun käytön, jonka tietoturvahaavoittuvuus vaarantaa luottamuksellisen tiedon turvallisuuden.

Tietoturvapoikkeamien raportointi ja käsittely

Jokaisen työntekijän ja Boltin tietoa käsittelevän henkilön velvollisuus on ilmoittaa havaitsemistaan tietoturvapoikkeamista ja –puutteista sekä epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista tietoturvapäällikölle tietoturva@bolt.works tai omalle esimiehelleen. Havaittuja poikkeamia hyödynnetään tietoturvallisten toimintatapojen, prosessien ja teknisten ympäristöjen kehittämisen tukena.

Mikäli poikkeamiin liittyy rikosepäily, päättää toimitusjohtaja tutkintapyynnön tekemisestä poliisille.

Fyysinen tietoturva

Boltin luottamuksellisten tietojen tallentamisessa pyritään takaamaan mahdollisimman hyvä tiedon suojaaminen fyysisiltä uhilta (kuten tulipalo, luonnonilmiöt jne), yritysvakoilun ja sabotaasin kaltaisilta uhilta ja vahingoilta. Lähtökohtaisesti tietoa ei tallenneta Boltin tiloissa oleville palvelimille tai laitteille, vaan ammattimaisesti ylläpidettyjen data centerien palvelimille, joiden fyysinen tietoturva, varmuuskopiointi, redundanssi, saavutettavuus ja kulunvalvonta ovat korkealla tasolla (kuten Amazon AWS).

Kulunvalvonta

Tiloihin, joissa säilytetään luottamuksellista tietoa (sähköisesti tai ei-sähköisesti) on järjestettävä kulunvalvonta.

Integriteetti ja varmuuskopiot

Luottamuksellisen tiedon integriteetti ja saatavuus on taattava varmuuskopioin ja suunnittelemalla tietojärjestelmäarkkitehtuuri siten, että se varmistaa riittävän redundanssin ja virheentarkistuksen (esim. RAID-levyjärjestelmä, palvelinten ja palveluiden kahdennus ja maantieteellinen hajautus). Missään realistisesti kuviteltavissa olevassa skenaariossa luottamuksellinen tieto ei saa suunnittelematta hävitä tai korruptoitua.

Saavutettavuus

Järjestelmät on suunniteltava niin, että luottamukselliseen tietoon on sen luonne huomioiden taattu pääsy ilman viivettä, joka haittaisi suoritettavien tehtävien suorittamista kohtuuttomasti. Esimerkiksi yrityksellä välttämättömän tiedon palauttaminen varmuuskopiolta ei saa kestää niin kauan, että se vaarantaa yrityksen toiminnan.

Valvonta, testaus ja auditointi

Kunkin tietojärjestelmän, tietovarannon tai palvelun tietoturvallisuuden toteutumisen seurannasta ja valvonnasta vastaa järjestelmän, aineiston tai palvelun omistaja.

Tietoturvan toteutumista yhtiössä valvotaan ulkopuolisten auditointien, sisäisen tarkastuksen ja katselmusten avulla. Teknistä tietoturvaa arvioidaan lisäksi jatkuvan teknisen valvonnan keinoin. Tärkeimpiin ympäristöihin ja järjestelmiin tehdään erillisiä tietoturvatarkastuksia auditointisuunnitelman mukaisesti. Yhtiön toiminnan kannalta kriittisiin järjestelmiin ja palveluihin tehdään tarvittaessa ulkopuolisen tai sisäisen arvioijan toimesta tietoturvatarkastus ennen tuotantoon ottoa ja sen jälkeen auditointisuunnitelman mukaisesti.

IT-osasto vastaa tietoverkkojen ja –järjestelmien valvonnasta niin sisäverkossa kuin verkon internet-rajapinnassa. Tietojärjestelmä- ja ohjelmistotoimittajien sekä viranomaisten ja muiden sopimuskumppaneiden haavoittuvuustiedottamista seurataan aktiivisesti. Ohjelmistohaavoittuvuuksia skannataan järjestelmistä säännöllisesti. Haavoittuvuuksien aiheuttamia riskejä ja vaikuttavauutta arvioidaan korjaustoimien perustaksi. Ulkoisten tietojärjestelmien valvonnan järjestelyt varmistetaan sopimuksilla.

Tietosuojavastaava valvoo ja seuraa tietosuojasäännösten, annettujen ohjeiden ja henkilötietojen käsittelyn asianmukaisuutta erillisen seuranta- ja valvontasuunnitelman mukaisesti.

Ulkopuolisten palvelutarjoajien prosessien ja järjestelmien auditointimahdollisuus varmistetaan sopimuksilla. Auditointeja tehdään riskiarvion perusteella kuitenkin vähintään kerran sopimuskauden aikana. Palveluntarjoajille asetettuja tietoturvavaatimuksia seurataan säännöllisesti asiakastapaamisissa.

Arkkitehtuurisuunnittelu ja –kuvaukset

Ennen toteuttamista kunkin tietojärjestelmän suunnittelussa huomioidaan tämän dokumentin vaatimukset. Tarvittaessa tietojärjestelmästä tehdään arkkitehtuurikuvaus, ja kuvaus, joka todentaa, miten järjestelmä toteuttaa tämän dokumentin vaatimukset.

Koulutukset, ohjeistukset, tiedottaminen ja tietoturvatietoisuuden ylläpito

Tietoturvakoulutus

Perehdytyksessä käsitellään aina tietoturvallisuuden perusperiaatteet ja salassa pidettävän tiedon käsittelyyn liittyvät yleiset periaatteet. Henkilöille, jotka käsittelevät salassa pidettävää tietoa tai henkilötietoja, annetaan erikseen tiedon luokitteluun ja käsittelyyn ohjaavaa koulutusta. Perehdytyksiin ja koulutuksiin osallistuneista henkilöstön jäsenistä pidetään kirjaa.

Tietoturvavastaava vastaa siitä, että henkilöstölle (ja soveltuvilta osin palveluiden käyttäjille) on tarjolla tietoturvaperehdytystä ja -koulutusta. Henkilöstön tietoturvaosaamisen tasoa soveltuvin menetelmin.

Ohjelmistokehityksen tietoturvaperiaatteet

Kaikessa Boltin ohjelmistokehityksessä noudatetaan seuraavia periaatteita:

- Kaikki luottamuksellinen tieto tulee suojata arkkitehtuurisin ratkaisuin niin, että minimoidaan riski sen integriteetin tai luottamuksellisuuden vaarantumiseen myös kuviteltavissa olevissa ohjelmointivirhe tai vikatilanteissa
- Tieto suojataan tarvittaessa kryptografisin keinoin ja mikäli mahdollista sitä ei tallenneta lainkaan selkokielisenä, kuten salasanat ja henkilötunnukset
- Kaikki salaus, tietoturvaratkaisut, haavoittuvuuksien ehkäisy jne tehdään kulloinkin vallitsevien parhaiden käytäntöjen mukaisesti
- Ulkoisen kirjastot ja palvelut pyritään valitsemaan siten, että niiden tietoturvataso on korkea, ja ne päivitetään aina kun tietoturva sitä vaatii
- Kaikessa toteutuksessa mietitään virheen ja ulkoisen uhan mahdollisuutta ja rakennetaan valmius torjua uhka.

Bolt-ohjelmiston tietoturva-arkkitehtuuri kuvataan erillisessä dokumentaatiossa.