# Öryggis- og viðbragðsáætlun vegna öryggisatvika

Snæfellsbær (hér eftir oftast nefnt „sveitarfélagið“) hefur skilgreint verklagsreglur um viðbrögð við atvikum sem tengjast upplýsingaöryggi og/eða persónuvernd. Er reglunum ætlað að ákvarða hvernig bregðast á við öryggisatvikum, óháð því hver uppruni atvikanna er.

## 1. Tilkynning um atvik

Starfsmenn og verktakar sveitarfélagsins skulu tilkynna um ætlað öryggisatvik um leið og það uppgötvast. Tilkynningum skal beint á netfangið personuvernd@snb.is. Starfsmenn geta jafnframt beint tilkynningu til næsta yfirmanns síns sem skal þá koma tilkynningu til öryggisstjóra með sannanlegum hætti.

Atvik geta verið öll frávik eða veikleikar sem geta haft áhrif á öryggi eða rekstur sveitarfélagsins, þ.á.m. öll frávik frá verklagsreglum og vinnureglum eða kerfum. Atvik geta falist í mistökum eða svikum starfsmanna. Atvik geta jafnframt legið í veikleikum í starfsaðstöðu eða aðgangsstýringum t.d. ólæst hurð eða gluggi, eða viðkvæm gögn eru skilin eftir óvarin. Ekki er um að ræða tæmandi talningu atvika.

## 2. Meðhöndlun atvika

1. Eftir að tilkynning hefur borist um öryggisatvik, hvort heldur það telst vera öryggisfrávik, öryggis veikleiki eða villur eða bilanir skal öryggisstjóri án tafar meta alvarleika atviksins. Hann getur kallað sér til aðstoðar hvern þann aðila, sem hann telur að nauðsynlegt er eða geti aðstoðað við að meta atvikið og ákveða viðbrögð, þ.m.t., persónuverndarfulltrúa, tæknifólk eða lögfræðing sveitarfélags. Tengist atvik meintum bresti á persónuvernd, er rétt að öryggisstjóri hafi samband við og setji persónuverndarfulltrúa inn í málið án ónauðsynlegra tafa. Sviðsstjóri þess svið sem atvikið varðar skal jafnframt upplýstur um atvikið án tafar.

2. Að öðru leyti er í reglum þessum ekki kveðið á um frekari verkskiptingu en öryggisstjóra er falið að velja þá aðila til verksins, sem best á við hverju sinni.

3. Strax og atburður hefur verið tilkynntur er æskilegt að eftirfarandi sé fylgt:

    a) greina og bera kennsl á orsök atviksins;
    b) ná tökum á atvikinu;
    c) skipuleggja og innleiða úrræði til þess að koma í veg fyrir endurtekningu eða stigmögnun, ef þörf krefur;
    d) takmarka aðgang á meðan úrræðum er hrint í framkvæmd;
    e) skjalfesta til hvaða úrræða var gripið;
    f) safna upplýsingum um úttektarslóðir og sambærilegum sönnunargögnum;
    g) kanna hvort og þá hvaða áhrif atvik eða úrræði hafi haft á aðra þætti í rekstri sveitarfélagsins;
    h) eftir því sem við á hafa samband við þá sem urðu fyrir áhrifum af atvikinu eða komu að endur bótum eftir atvikið;
    i) útbúa skýrslu um aðgerðir sem síðan er skoðuð sem hluti af innra eftirliti og eftir því sem við á send persónuverndarfulltrúa og Persónuvernd.

4. Leitast skal við að halda utan um úttektarslóðir og sambærileg sönnunargögn og varðveita þau eftir því sem við á.

5. Aðgerðir sem miða að því að rétta við eftir öryggisatvik skulu vera undir formlegri stýringu og skjalfestar.

6. Reglulega skal fara yfir skráð atvik til að uppgötva frávik frá öryggisreglum, ástæður þeirra og hvort hægt sé að draga lærdóm af þeim.

## 3. Tilkynning til Persónuverndar um öryggisbrest við meðferð persónuupplýsinga

1. Ef um öryggisbrest við meðferð persónuupplýsinga er að ræða skal sveitarfélagið, án ótilhlýðilegrar tafar, og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brestsins var, tilkynna Persónuvernd, sem er lögbært skv. 55. gr., um hann nema ólíklegt þyki að bresturinn leiði til áhættu fyrir rét tindi og frelsi einstaklinga. Sé Persónuvernd ekki tilkynnt um brestinn innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni.

2. Öryggisbrestur við vinnslu persónuupplýsinga er skilgreindur sem: Brestur á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga eða þess að þær glatist, breytist, verði birtar eða aðgangur verði veittur að þeim í leyfisleysi.

3. Við mat á eðli öryggisatviks og hvort um sé að ræða tilkynningarskyldan öryggisbrest í skilningi laga um persónuvernd nr. 90/2018, skal notast við leiðbeiningar útgefnar af Persónuvernd á árinu 2018, sbr. fskj. nr. 1.

4. Vinnsluaðili skal tilkynna sveitarfélaginu og persónuverndarfulltrúa um það án ótilhlýðilegrar tafar ef hann verður var við öryggisbrest við meðferð persónuupplýsinga.

5. Í tilkynningunni, sem um getur í lið 1, skal a.m.k.:

   a) lýsa eðli öryggisbrests við meðferð persónuupplýsinga, þ.m.t., ef hægt er, þeim flokkum og áætluðum fjölda skráðra einstaklinga sem hann varðar og flokkum og áætluðum fjölda skráa með persónuupplýsingum sem um er að ræða,

   b) gefa upp nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar,

   c) lýsa líklegum afleiðingum öryggisbrests við meðferð persónuupplýsinga,

   d) lýsa þeim ráðstöfunum sem sveitarfélagið hefur gripið til eða fyrirhugar að grípa til vegna öryggisbrests við meðferð persónuupplýsinga, þ.m.t., eftir því sem við á, ráðstöfunum til að milda hugsanleg skaðleg áhrif hans.

   e) Notast skal við eyðublað sem Persónuvernd hefur aðgengilegt á heimasíðu sinni vegna tilkynninga um öryggisbrest, sbr. fskj. nr. 2.

6. Ef, og að því marki sem, ekki er mögulegt að láta upplýsingarnar í té á sama tíma er heimilt að veita þær í áföngum án ástæðulausra frekari tafar.

7. Sveitarfélagið skal skrá niður hvers kyns öryggisbresti við meðferð persónuupplýsinga og tilgreina málsatvik í tengslum við viðkomandi brest, áhrif hans og aðgerðir til úrbóta sem gripið var til. Þessi skráning skal gera Persónuvernd kleift að sannreyna að farið sé að ákvæðum þessarar greinar.

## 4. Skráðum einstaklingi gert viðvart um öryggisbrest við meðferð persónuupplýsinga

1. Ef líklegt er að öryggisbrestur við meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga skal þá tilkynna skráðum einstaklingi um brestinn án ótilhlýðilegrar tafar.

2. Í tilkynningunni til hins skráða skal lýsa á skýru og einföldu máli eðli öryggisbrests við meðferð persónuupplýsinga og skal hún a.m.k. innihalda þær upplýsingar og ráðstafanir sem um getur í lið 3) b-, c- og d í grein 3 að ofan.

3. Þess skal ekki krafist að skráðum einstaklingi sé gert viðvart ef eitthvert eftirtalinna skilyrða er uppfyllt:

   a) Sveitarfélagið hefur gert viðeigandi tæknilegar og skipulagslegar verndarráðstafanir og þessar ráðstafanir voru gerðar varðandi þær persónuupplýsingar sem öryggisbrestur við meðferð

   b) persónuupplýsinga hafði áhrif á, einkum ráðstafanir til að gera persónuupplýsingar óaðgengilegar hverjum þeim sem ekki hefur aðgangsheimild að þeim, s.s. með dulkóðun.

   c) Sveitarfélagið hefur gert ráðstafanir í kjölfarið sem tryggja að ólíklegt sé að aftur komi til jafnmikillar áhættu fyrir réttindi og frelsi skráðra einstaklinga og um getur í lið 2),

   d) það myndi hafa í för með sér óhóflega fyrirhöfn. Í því tilviki skal í staðinn birta almenna tilkynningu eða grípa til svipaðrar ráðstöfunar þar sem hinum skráðu er gert viðvart með jafn áhrifaríkum hætti.

## Viðhald verklagsreglu

Sviðsstjóri og öryggisstjóri.

## Fylgiskjöl

1. Leiðbeiningar um tilkynningar um öryggisbrot útgefið af Persónuvernd 2018.

2. Eyðublað til tilkynningar á öryggisbrest. Birt og aðgengilegt á heimasíðu Persónuverndar.

## Endurskoðun

Þessi verklagsregla endurskoðast í síðasta lagi: 01.05.2021.