Mikilvægi öryggisstefnu

- Það sem áður var viðfangsefni annarra er nú orðið mitt

Guðmundur Stefán Björnsson
Sensa – gsb@sensa.is

sensa

bsi. ISO/IEC 27001 Information Security Management
IS 602023

15 ára

Til hvers öryggisstefna?

Hún er mikilvæg þar sem tryggja þarf öryggi

- Mannauður
- Innviðir samfélagsins
- Samgöngur
- Náttúruhamfarir
- Upplýsingaöryggi
- .....
- Persónugreinanlegar upplýsingar

sensa

Öryggisstefna – skýr og einföld

Hvað er það sem verið er að verja
Hvernig ætlum við að tryggja framgang hennar
    Markmið
Hvernig mælum við árangurinn
    T.d. reglulegt áhættumat
Lýsa umfanginu ef svo ber undir
    Umfangið þarf að ná yfir það sem henni er ætlað
    …getur verið flókið - dæmi á næstu glæru
Starfsmenn og viðskiptavinir þurfa að „tengja“

Mikið efni til um þetta á netinu….Googla

Linkur á stefnu

sensa

Upplýsingaöryggisstefna

Sensa fylgir eftirfarandi upplýsingaöryggisstefnu sem nánar er lýst í skjali um stjórnun upplýsingaöryggis. Við mótun stefnunnar og stjórnkerfisins var hafður til hliðsjónar staðallinn *ISO/IEC 27002 – Starfsvenjur fyrir stjórnun upplýsinga.*

1. Sensa skuldbindur sig til að hámarka öryggi upplýsinga í vörslu fyrirtækisins m.t.t. leyndar, réttleika og tiltækileika.
2. Sensa fylgir lögum, reglum og leiðbeiningum um stjórnun upplýsingaöryggis sem eru grundvöllur skipulags og viðhalds ráðstafana til að standa vörð um leynd, réttleika og tiltækileika gagna og upplýsingakerfa.
3. Stefna Sensa í upplýsingaöryggismálum er bindandi fyrir alla starfsmenn fyrirtækisins og nær til allra sem veita Sensa þjónustu.
4. Allir starfsmenn, verktakar og þjónustuaðilar Sensa eru skuldbundnir til að vernda gögn og upplýsingakerfi gegn óheimilum aðgangi, notkun, breytingum, uppljóstrun, eyðileggingu, tapi eða flutningi.
5. Sensa stuðlar að virkri öryggisvitund starfsmanna, þjónustuaðila, viðskiptavina og gesta.
6. Sensa tryggir að öllum þáttum þessarar stefnu sé framfylgt með ráðstöfunum í samræmi við störf og ábyrgð viðkomandi einstaklinga.
7. Sensa framkvæmir árlega áhættugreiningu á öllum verðmætum fyrirtækisins, metur aðgerðir úr frá áhættustigi og samþykkir. Áhættumat er einnig framkvæmt ef breytingar verða á innra umhverfi, ný kerfi tekin í notkun eða alvarleg frávik verða sem leiða af sér endurmat á áhættustigi.
8. Árlega er gerð skýrsla varðandi framkvæmd og virkni öryggisstefnu Sensa.
9. Starfsmönnum og þjónustuaðilum, núverandi og fyrrverandi, er óheimilt að veita upplýsingar um málefni Sensa, viðskiptamanna þess eða annarra starfsmanna.
10. Sensa endurskoðar þessa stefnu eins og tilefni er til en að lágmarki á tveggja ára fresti.
11. Sensa mun hlíta *ISO/IEC 27001: 2013 – Stjórnunarkerfi fyrir upplýsingaöryggi* sem eru grundvöllur skipulags- og viðhaldsaðgerða til að standa vörð um *leynd, réttleika* og *tiltækileika* gagna og upplýsingakerfa.

Umfang

Stjórnkerfi upplýsingaöryggis hjá Sensa nær til innri starfsemi fyrirtækisins, húsnæðis og rekstrarþjónustu sem Sensa veitir viðskiptavinum sínum á samnýttum eða sértækum búnaði, auk allra innri kerfa, hug- og vélbúnaðar í eigu og undir fullri stjórn Sensa.

The scope of the ISMS covers all internal operations, housing and managed services which Sensa provides to customers on shared or specific equipment, as well as all internal systems, software and hardware owned and solely operated by Sensa.

Dæmi – Umfang ISO vottunar Sensa

Stjórnkerfi upplýsingaöryggis hjá Sensa nær til innri starfsemi fyrirtækisins, húsnæðis og rekstrarþjónustu sem Sensa veitir viðskiptavinum sínum [redacted], bæði á samnýttum og sértækum búnaði

Þessi hluti setningarinnar „útilokaði“ eitt mesta virði Sensa sem er rekstrarþjónusta gagnvart búnaði v.v.

Það sem áður var viðfangsefni annarra er nú orðið mitt

?

GDPR – nýju persónuverndarlögin

sensa

15 ára

Hvað breytist?

Ný reglugerð ber með sér nýjar og auknar skyldur

Tekur gildi í Evrópu í maí 2018

Skerpt á skyldum ábyrgðaraðila og vinnsluaðila

Réttur til að gleymast

……

ALVARLEG BROT GETA NUMIÐ ALLT AÐ 4% AF VELTU FYRIRTÆKIS / SAMSTEYPU

sensa

Persónuupplýsingar

Rekja má beint eða óbeint til tiltekins einstaklings, látins eða lifandi

Nöfn, kennitölur, heimilisföng……

Samhengi gagnanna sem leiðir af sér persónugreiningu

sensa

Þar sem verið er að sýsla með persónugreinanleg gögn þarf að huga að….

Öryggisstefnu
eða
Persónuverndarstefnu

……..hefur ekki verið á „radarnum“ hjá minni fyrirtækjum

Af hverju núna? Hefur þetta ekki alltaf verið?

.....núna er verið að „sverfa til stáls“

sensa

Hver kannast ekki við….

……lítið land, „allir þekkja alla“

sensa

15 ára

Hvernig nálgaðist Sensa GDPR?

- Lá ekki ljóst fyrir í upphafi hvernig ætti að nálgast
- Nálgast út frá verðmætum
  - Hvernig vinnsla (hýsing, öryggi, umsýsla, flutningur)
  - Ábyrgð (ábyrgðaraðili, vinnsluaðili)
  - Er um að ræða flutning utan Evrópu
  - Er um að ræða persónugreinanleg gögn
  - …og þá hvernig gögn (nafn, símaumferð, IP tölur….)

sensa

Þar sem um er að ræða persónugreinanleg gögn

- Kortlagning upplýsinga og rafrænnar vöktunar um starfsmenn, verktaka, viðskiptavini
  1. Tegund, hvern varðar, uppruni
  2. Varðveislutími- og aðferð
  3. Tilgangur og heimild
  4. Hversu viðkvæmar
  5. Ábyrgðaraðili, vinnsluaðili
  6. Aðgangur
  7. Fræðsla
- Áhættumat – yfirfara sérstaklega m.t.t. GDPR

sensa

15 ára

Áskorunin

Tækifæri að færa upp á yfirborðið – með starfsfólkinu

Fá aðstoð

Þjálfun starfsmanna

- Móta saman (hópurinn) stefnuna
- Regluleg vitundarvakning (innri eða ytri)
- Leiðbeiningar – kvitta fyrir lestur
- Mæla árangurinn – saman

…rúlla boltanum af stað

Það sem áður var viðfangsefni annarra er nú orðið mitt

sensa