

## Upplýsingaöryggisstefna

Fyrirtækið 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. Félagið skuldbindur sig til að hámarka öryggi upplýsinga í vörslu fyrirtækisins m.t.t. leyndar, réttleika og tiltækileika.
2. Fyrirtækið 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 í upplýsingaöryggismálum er bindandi fyrir alla starfsmenn fyrirtækisins.
4. Starfsmenn, auk verktaka og þjónustuaðila sem hafa aðgengi að rými og/eða upplýsingum Sensa, eru skuldbundnir til að vernda gögn og upplýsingakerfi gegn óheimilum aðgangi, notkun, breytingum, uppljóstrun, eyðileggingu, tapi eða flutningi.
5. Fyrirtækið stuðlar að virkri öryggisvitund starfsmanna, þjónustuaðila, viðskiptavina og gesta.
6. Félagið tryggir að stefnunni sé framfylgt með ráðstöfunum í samræmi við störf og ábyrgð viðkomandi einstaklinga.
7. Árlega er framkvæmd áhættugreining á öllum verðmætum fyrirtækisins, lagðar til aðgerðir út frá áhættustigi og þær samþykktar. Áhættumat er einnig gert við framkvæmd breytinga, þegar ný kerfi eru tekin í notkun og við alvarleg frávik. Jafnframt er sett fram dagskrá fyrir hvert ár yfir innri úttektir. Þannig er stuðlað að stöðugum umbótum í rekstri félagsins.
8. Í upphafi árs er gerð skýrsla um árangur af rekstri stjórnkerfisins. Fjallað er um helstu lykiltölur og markmið ásamt því að setja ný markmið fyrir komandi ár.
9. Starfsmönnum og þjónustuaðilum, núverandi og fyrrverandi, er óheimilt að veita upplýsingar um málefni fyrirtækisins, starfsmanna eða viðskiptamanna til þriðja aðila nema að fengnu samþykki ábyrgðaraðila.
10. Framkvæmdastjóri er eigandi upplýsingaöryggisstefnunnar og á ábyrgð framkvæmdastjórnar að henni sem framfylgt. Stefna þessi er endurskoðuð a.m.k. á þriggja ára fresti og er á ábyrgð öryggisstjóra að framkvæma.
11. Félagið 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

Afhending stafrænnar þjónustu og þjónusta við viðskiptavini / Delivery of Digital Transformation services and Support function.

Reykjavík 5. desember 2023

---

Valgerður Hrund Skúladóttir, Framkvæmdastjóri