Icelandic (Original)

Upplýsingaöryggisstefna Primex ehf.

Útgefið: 24. janúar 2025

UPPLÝSINGAÖRYGGISSTEFNA PRIMEX EHF.

TILGANGUR OG UMFANG

Upplýsingaöryggisstefna félagsins lýsir áherslum stjórnenda Primex ehf. í upplýsingavernd og öryggi í upplýsingavinnslu. Verja þarf upplýsingaeignir félagsins fyrir öllum ógnum, innri og ytri, af ásetningi, vegna óhappa eða af slysni. Fagleg samræmd vinnubrögð eru lykillinn að árangri og til marks um það er þessi upplýsingaöryggisstefna sett. Innleiðing og framkvæmd stefnunnar er mikilvæg til að starfsemi og þjónusta fyrirtækisins sé sem öruggust og rétt vinnubrögð viðhöfð.

Upplýsingaöryggisstefna Primex ehf. tekur til öryggis á upplýsingaeignum félagsins og til allra upplýsinga í hvaða formi sem er og á hvaða miðli sem er. Stefnan tekur til umgengni, meðhöndlunar og varðveislu gagna í hvaða formi sem er og þeirra vinnuferla sem lúta að þjónustu og starfsemi á öllum starfsstöðvum Primex.

Upplýsingaöryggisstefnan tekur jafnframt til húsnæðis og búnaðar þar sem upplýsingar eru meðhöndlaðar eða vistaðar sem og starfsmanna og samningsbundinna verktaka sem hafa aðgang að upplýsingum félagsins og starfsstöðvum Primex.

STEFNA

Primex skal stuðla að öryggi upplýsingaverðmæta með skipulögðu verklagi sem styður við samfelldan rekstur og lágmarkar rekstraráhættu.

English (Translation)

Information Security Policy of Primex ehf.

Published: 24 January 2025

INFORMATION SECURITY POLICY OF PRIMEX EHF.

PURPOSE AND SCOPE

The Information Security Policy of Primex ehf. (“the Company”) outlines the emphasis of the Company’s management on information protection and data security. The Company’s information assets must be protected against all threats, internal and external, deliberate or accidental. Professional and standardized practices are the key to success, and this policy has been established to demonstrate that commitment. The implementation and execution of the policy are vital to ensure that the Company’s operations and services are as secure as possible and that proper working procedures are followed.

The Information Security Policy of Primex ehf. applies to the security of the Company’s information assets and to all forms of information, regardless of format or medium. The policy covers the handling, management, and storage of data, as well as all work processes related to services and operations at all Company sites.

The Information Security Policy also applies to the facilities and equipment where information is processed or stored, as well as to employees and contractors who have access to the Company’s information or sites.

POLICY

Primex shall promote the security of its information assets through organized procedures that support business continuity and minimize operational risk.

MARKMIÐ

Markmið Primex ehf. með upplýsingaöryggisstefnunni eru að:

1. Tryggja hámarks öryggi upplýsingaverðmæta ásamt upplýsingakerfa í eigu eða umsjón félagsins.

2. Verja upplýsingaverðmæti gegn óheimilum aðgangi, óviðeigandi notkun, uppljóstrun eða eyðingu á mikilvægum og viðkvæmum gögnum.

3. Áþreifanlegt öryggi sé tryggt á starfsstöðum félagsins og athafnasvæðum þess.

4. Koma á og viðhalda virkri vitund um upplýsingaöryggi hjá starfsmönnum og stjórn og þeim sem fá aðgang að upplýsingaverðmætum í starfi sínu fyrir félagið.

5. Stöðug og markviss vinna sé innan félagsins til að stuðla að umbótum og framkvæma reglulegt mat á áhættu svo hægt sé að meta hvort þörf sé á úrbótum á upplýsingaöryggi félagsins.

LEIÐIR AÐ MARKMIÐUM

Leiðir Primex ehf. að ofangreindum markmiðum eru að:

• Halda skrá yfir upplýsingaeignir félagsins og flokka þær eftir mikilvægi í rekstri þess.

• Greina reglulega, með formlegu áhættumati, verðmæti upplýsingaeigna, viðkvæmni þeirra og ógnir sem geta stefnt þeim í hættu.

• Greina reglulega, með formlegu áhættumati, aðgengi að starfsstöðvum félagsins og eignum, viðkvæmni þeirra og ógnir sem geta stefnt þeim í hættu.

• Starfsmenn og þjónustuaðilar fái þjálfun og fræðslu varðandi upplýsingaöryggi og ábyrgð þeirra hvað það varðar.

OBJECTIVES

The objectives of Primex ehf. with this Information Security Policy are to:

1. Ensure maximum security of information assets and information systems owned or managed by the Company.

2. Protect information assets from unauthorized access, inappropriate use, disclosure, or destruction of important and sensitive data.

3. Ensure physical security at the Company's sites and operational areas.

4. Establish and maintain active awareness of information security among employees, management, and those who access information assets as part of their work for the Company.

5. Maintain a continuous and systematic effort within the Company to promote improvement and regularly assess risk to determine whether improvements to information security are needed.

MEANS TO ACHIEVE OBJECTIVES

The Company's methods for achieving these objectives are to:

• Maintain an inventory of information assets and classify them by their importance to the Company's operations.

• Regularly, through formal risk assessments, identify the value, sensitivity, and potential threats to information assets.

• Regularly, through formal risk assessments, review access to the Company's facilities and assets, their vulnerabilities, and the threats that could endanger them.

• Ensure employees and service providers receive training and education on information security and their responsibilities in this regard.

• Fylgja öllum samningum sem fyrirtækið er aðili að og varða upplýsingaöryggi.	• Comply with all contracts related to information security to which the Company is a party.
• Áætlanir séu gerðar um samfelldan rekstur, þeim sé viðhaldið og þær prófaðar eins og kostur er.	• Prepare, maintain, and test business continuity plans as far as practicable.
• Frávik, brot eða grunur um veikleika í upplýsingaöryggi séu tilkynnt og rannsökuð.	• Report and investigate deviations, breaches, or suspected weaknesses in information security.
• Að áhætta vegna vinnslu (meðferðar) og varðveislu upplýsinga sé innan skilgreindra áhættumarka.	• Ensure that risk arising from the handling and storage of information remains within defined risk limits.
ÁBYRGÐ Ábyrgð við framkvæmd og viðhald upplýsingaöryggisstefnunnar skiptist á eftirfarandi hátt:	RESPONSIBILITY Responsibility for implementing and maintaining this Information Security Policy is divided as follows:
• Framkvæmdastjórn Primex ber ábyrgð á upplýsingaöryggisstefnunni og endurskoðun hennar.	• The Executive Management of Primex is responsible for the policy and its review.
• Framkvæmdastjórn Primex ber ábyrgð á framkvæmd upplýsingaöryggisstefnunnar og beitir til þess viðeigandi verklags- og vinnuferlum.	• The Executive Management of Primex is responsible for the execution of the policy and for applying the appropriate procedures and processes to do so.
• Framkvæmdastjórn Primex ber ábyrgð á því að gerðir séu samningar við verktaka og birgja svo framkvæmd stefnunnar sé fylgt.	• The Executive Management of Primex is responsible for ensuring that contracts are made with contractors and suppliers to ensure compliance with this policy.
• Framkvæmdarstjórar bera ábyrgð á þeim upplýsingaverðmætum sem til verða í viðkomandi rekstrareiningu og að starfsmenn fari eftir þeim reglum og tilmælum sem gilda um öryggi upplýsinga.	• Division managers are responsible for the information assets generated within their operating unit and for ensuring that employees follow the applicable rules and guidelines on information security.
• Stjórnendur Primex setja reglur um aðgengi starfsmanna og samningsbundinna verktaka að starfsstöðvum félagsins.	• Company managers set the rules governing employee and contractor access to Company facilities.
• Allir starfsmenn Primex bera ábyrgð á að þeim verklags- og vinnuferlum sem eiga að tryggja framkvæmd upplýsingaöryggisstefnunnar, sé fylgt.	• All employees of Primex are responsible for following the procedures and processes that ensure the implementation of this policy.

• Starfsmenn Primex skulu ábyrgjast að framkvæmd reglna um aðgengi viðskiptamanna, verktaka og birgja að starfsstöðvum félagsins sé með þeim hætti að hún tryggi að framkvæmd stefnunnar sé fylgt.

• Öllum starfsmönnum Primex ber að vinna samkvæmt upplýsingaöryggisstefnunni. Þeim ber að tilkynna öryggisfrávik og veikleika sem varða upplýsingaöryggi. Þeir sem ógna upplýsingaöryggi Primex eða viðskiptavina hans af ásettu ráði eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir.

Þannig samþykkt af stjórn þann 23. janúar 2025.

• Employees of Primex shall ensure that the implementation of access rules for customers, contractors, and suppliers to Company facilities is conducted in such a way that compliance with this policy is maintained.

• All employees must comply with this Information Security Policy. They must report security deviations and weaknesses relating to information security. Those who deliberately compromise the information security of Primex or its clients are subject to prosecution or other appropriate legal action.

Approved by the Primex Board of Directors on 23 January 2025.