TRYGGINGAMIÐLUN ÍSLANDS ehf
Hlíðamára 12, 201 Kópavogur
Sími: 553 6688 Fax: 581 1805
Netfang: tmi@tmi.is ww.tmi.is

Tryggingamiðlun Íslands ehf Information Security and Data Protection Policy

1. Introduction

This Information Security and Data Protection Policy outlines the principles, procedures, and measures to protect information assets and ensure compliance with the General Data Protection Regulation (GDPR) within Tryggingamiðlun Íslands ehf. (TMI). This policy aims to safeguard the confidentiality, integrity, and availability of personal data and other sensitive information.

2. Information Security Principles

Confidentiality: Information, especially personal data, is handled with the utmost confidentiality, and access is restricted to authorised personnel only.

Integrity: Measures are in place to ensure the accuracy and completeness of information, preventing unauthorised alterations.

Availability: Information systems and data are available and accessible to authorised users when needed.

Compliance: TMI shall comply with applicable laws, regulations, and contractual obligations related to information security and data protection.

3. Data Classification and Handling

Information, including personal data, is classified based on sensitivity, and appropriate security controls are implemented according to the classification. Clear procedures are established for the proper handling, storage, and transmission of different classifications of information.

4. Access Controls

Access to systems and data are granted on a need-to-know basis. Strong authentication mechanisms, including multi-factor authentication, is implemented for access to sensitive systems and data. Regular reviews of user access rights are conducted to ensure appropriateness and necessity.

5. Password Policy

A strong password policy is in place, which includes the use of complex passwords and regular password changes.

TRYGGINGAMIÐLUN ÍSLANDS ehf
Hlíðamára 12, 201 Kópavogur
Sími: 553 6688 Fax: 581 1805
Netfang: tmi@tmi.is ww.tmi.is

6. **Data Breach Response and Notification**

A comprehensive incident response plan is in place to detect, respond to, and recover from security incidents, including data breaches.

In the event of a data breach, TMI complies with GDPR notification requirements, including notifying the relevant supervisory authority and affected data subjects, where applicable.

7. **Third-Party Management**

Third-party service providers are assessed for their information security and data protection practices before engagement. Contracts with third parties shall include provisions ensuring they adhere to the same information security and data protection standards as TMI.

8. **Training and Awareness**

All personnel receive training on information security, data protection, and GDPR compliance. Regular awareness programs are conducted to keep employees informed about the latest threats and best practices.

9. **Data Protection Officer (DPO)**

A designated DPO is responsible for overseeing compliance with GDPR and ensuring effective implementation of data protection measures.

This Information Security and Data Protection Policy is regularly reviewed to ensure its alignment with the latest GDPR requirements and updates in the regulatory framework.

Kópavogur – 30 December 2025

Atli Már Ólafsson – Compliance Officer.