progressive

Policy for Information Security

+45 35 25 50 70 info@progressive.dk Lyskær 3B, 2730 Herlev Søndervangs Alle 20, 8260 Viby J

PURPOSE

The Policy for Information Security is intended to support and promote Progressive's vision and mission. It is implemented and administered with respect to Progressive's key values.

The objective of the Information Security Policy is to make sure everyone with a relationship to Progressive and any of its subsidiaries knows that the use of information and information systems are subject to standards and guidelines.

Maintenance and development of a high level of security is crucial, if Progressive is to be considered trustworthy both nationally and internationally.

In order to maintain Progressive's credibility, every reasonable step must be taken to ensure that Progressive's customers information as well as Progressive's own information is handled with the requisite confidentiality and that data is handled precisely and promptly.

SCOPE

After Progressive's staff, IT systems are considered the most critical resource. Great importance is therefore attached to operational reliability, quality, observance of legal requirements and ensuring that the systems are user-friendly, i.e. without unnecessarily inconvenient security measures.

An appropriate protection level for Progressive, its subsidiaries and Progressive's customers are established against information security-related threats. This protection must be aimed at natural, technical, and human-induced threats.

Information security in Progressive is defined as the practice of protecting and mitigating threats to information processing facilities to uphold data confidentiality, integrity, and availability. Progressive implements all requisite activities to ensure:

- **Confidentiality:** To establish the possibility for confidential handling, transmission and storage of data to which only authorized and authenticated users have access
- **Integrity:** To achieve proper functioning of the systems with a minimal risk of manipulation of, data loss and errors in, both data and systems.
- **Availability:** To achieve a high degree of availability with high up-times and a minimal risk of major breakdowns.

This information security policy is governing the entirety of Progressive and its subsidiaries, which means that the below companies, brands and employees employed at any of them, is subject to this policy:

This Policy for Information Security applies to all of Progressive's information processing facilities and information-related activities, regardless of which company or brand any employee is employed with

PRINCIPLES

Information security at Progressive and its subsidiaries is implemented in accordance with the following overall positions:

1. Progressive develops, implements, and maintains an Information Security Management System that underpins and correlates to our business strategy based on the controls, safeguards and regulations of the ISO 27001 Standard and EU General Data Protection Regulations.
2. Progressive performs internal audits and assessments based on the ISO 27001 Standard and EU General Data Protection Regulations to uphold an adequate level of information security.
3. Progressive commits to yearly undergo independent and external audits based on the ISAE 3402 and ISAE 3000.
4. Progressive minimizes its risks of security incidents by identifying and mitigating vulnerabilities and risks through Risk Management facilities.
5. Progressive ensures the protection of all data we are responsible for, including the protection of intellectual property and sensitive data such as personally identifiable information (PII).
6. Progressive ensures compliance with contractual and regulatory requirements such as the EU General Data Protection Regulation and other relevant contractual and regulatory requirements.
7. Progressive commits to uphold and ensure an adequate amount of resources to uphold this information security policy.
8. Progressive ensures to place the responsibility of information security at the senior management level and ensures that the Information Security Management System is performing effectively and as intended.
9. Progressive expects its employees and business partners to have a healthy and critical position towards information security and the protection of information processing facilities.
10. Progressive has a standardized and uniform governance structure in all of its subsidiaries in regard to its information security policies and principles.
11. Progressive ensures quick response and commitment to mitigating the damage caused by security incidents.
12. Progressive ensures to assess and enforce an adequate level of information security with our suppliers to ensure that our suppliers are subject to the same high standards for information security as Progressive.
13. Progressive uses a standardized framework, governance model, documents and systems for ISMS and PIMS in Progressive and its subsidiaries.

ORGANIZATION & RESPONSIBILITIES

The Security related responsibilities and its authority are based on roles in the organization and are described in the Information Security Management System (ISMS).

Progressive centralizes the main authority for the Information Security Management System around the group function Compliance & Security to ensure a high level of compliance with regulatory and contractual requirements, support in the continuous maturing of information security in all Progressive brands and the synergy of information security initiatives across the entire group.

Employees who breach valid information security initiatives in effect at Progressive may face disciplinary actions. On the basis of an individual assessment of the breach, it may be perceived as a violation of the terms of employment.

REFERENCES

- International Organization for Standardization ISO/IEC 27001:2017
- EU General Data Protection Regulation

MANAGEMENT APPROVAL & SIGNATURE

Date:

_____