Deutsche Post DHL Group

DEUTSCHE POST DHL GROUP

INFORMATION SECURITY POLICY

Document Owner: DPDHL Group CISO

Version 2– 2022 Spring

PUBLIC

TABLE OF CONTENT

1 MISSION STATEMENT FOR INFORMATION SECURITY AT DEUTSCHE POST DHL GROUP

1.1 Commitment to Information Security

The Corporate Board of Deutsche Post DHL Group fully commits itself to appropriately protecting the information of Deutsche Post DHL Group and that of our customers, partners, and employees.

As the world's leading logistics provider, we implement Information and Cyber Security measures to protect our businesses around the globe. In doing so, we strive to prevent disruption of business operations and related damage as well as to comply with relevant laws and legislation.

Securing and protecting information supports Deutsche Post DHL Group's goal of being Provider, Employer, and Investment of Choice. This enables Deutsche Post DHL Group to meet our customers' expectations and maintain our investors' trust, promoting growth in both existing and new markets, and to keep our employees' information private and secure.

1.2 Approach to Information Security

The Corporate Board of Deutsche Post DHL Group ensures that Information Security is promoted, implemented and managed consistently across the Group by establishing a dedicated Information Security organization, who defines standards and supporting processes, which are instantiated and implemented throughout Deutsche Post DHL Group.

Within Deutsche Post DHL Group, Information Security is based upon:

- Ensuring adequate levels of protection by implementing appropriate governance, processes and technologies following a risk-based approach.
- Referencing all Information Security related activities to internationally recognized good practices and standards.
- Promoting continuous improvement of Information Security activities using our First Choice methodologies.
- Engaging our employees as an essential part of our defense.

1.3 Governance of Information Security

The Corporate Board of Deutsche Post DHL Group has resolved that Information Security is governed through an Information Security Management System specified and documented in the Information Security Target Model and is implemented across Deutsche Post DHL Group.

The Information Security Target Model delivers a systematic approach to planning, adopting, implementing, supervising, and improving tasks and activities needed to protect information by leveraging people, processes, and information systems and by applying a risk management process. It addresses the following components:

1. Management of the Information Security Management System to ensure that all of its parts are implemented across the Group, to define Information Security requirements, and to ensure that the Information Security organization functions appropriately.

2. Information Security Risk Management to identify, assess and mitigate risks and exploit opportunities using defined risk assessment criteria, and with unambiguously identified risk owners who approve the risk treatment plan and accept residual risk.
3. Information Security Measurement and Reporting to monitor, measure, analyze, and evaluate the effectiveness of the Information Security Management System. Metrics are used to improve the Information Security Management System and the technological environment, allowing management to make informed decisions.
4. Information Security Incident Management to ensure effective handling and communication of Information Security events and incidents, to resolve them in a timely manner with minimum disruption, to preserve evidence as required, and to improve capabilities, processes, and technologies from lessons learned.
5. Information Security Awareness, Education, Training, and Practice to enable our employees to properly identify and treat Information Security risks in the best interest of Deutsche Post DHL Group.

The following rules for accountability and responsibility apply:

	Group Level	**Divisional Level**
Accountability and responsibility for business impact	Corporate Board	Business Owner
Accountability for Information Security	IT Board	Divisional Chief Information Officer (CIO)
Responsibility for Information Security	Information Security Committee	Divisional Chief Information Security Officer (CISO)

The financial, strategic, and operational needs of Deutsche Post DHL Group as well as legal and ethical standards determine the objectives to be achieved within Information Security. These objectives are measured to ensure that the intended goals are achieved within the appropriate timeframe.

2 SCOPE OF INFORMATION SECURITY

2.1 Control Set Reference

The Corporate Board of Deutsche Post DHL Group makes the voluntary commitment that the Information Security Target Model complies with International Standard Organization ISO/IEC 27001:2013.

2.2 Statement of Applicability

Information Security at Deutsche Post DHL Group aims to protect all assets belonging to Deutsche Post DHL Group from Information and cyber security related threats. This includes, but is not limited to, customer data, financial data, and employee data, applications, storage and computing devices, networks, and physical assets.

The Information Security Target Model is valid and binding for all personnel of Deutsche Post DHL Group and for suppliers and partners who must meet or exceed its requirements. The Information Security Target Model further addresses Customers, Investors, Government Authorities, and the Public.

2.3 Protection Objectives

Protecting from Information Security related threats means preserving the confidentiality, integrity, and availability of information, which is understood as follows:

- **CONFIDENTIALITY:** Ensuring that information is accessible only to authorized individuals, entities or processes.
- **INTEGRITY:** Ensuring the accuracy and completeness of information over its entire lifecycle.
- **AVAILABILITY:** Ensuring that only authorized individuals, entities, or processes have timely and uninterrupted access to an information at all required times.

3 GUIDING PRINCIPLES OF INFORMATION SECURITY

These Guiding Principles define how to establish, implement, maintain, and continuously improve the Information Security Management System.

3.1 Managing, Implementing, and Supporting Information Security

The management directly accountable for Information Security ensures that personnel of appropriate competence and in the required quantity is and remains staffed.

Information Security roles and responsibilities are identified, defined, and established.

Employees of Deutsche Post DHL Group need to be aware of the Information Security Target Model, of how to support the Information Security Management System, and of the consequences of not implementing it. These awareness needs and all other information relevant to the successful implementation of the Information Security Management System need to be continuously communicated.

Suppliers and partners are to ensure adequate and appropriate Information Security measures for the products and/or services that they provide. The required level of Information Security will be determined by means of a risk assessment, which is evaluated by members of the Information Security organization.

3.2 Monitoring and Measuring the Effectiveness of Information Security

The effectiveness and efficiency of Information Security related activities inside and outside of the Information Security Management System are measured and monitored continuously with the support of appropriate methodologies and technologies.

Information Security assessments, measuring effectiveness and efficiency, are performed following a defined plan that details scope, methodology, frequency, and entity.

The results of measurement and monitoring are duly analyzed by the Information Security organization, and provide input to management and may lead to technical, organizational, and procedural changes.

Effectiveness and efficiency of the Information Security Management System, as well as analysis and evaluation of the current risk level and of the threat environment, and the outcome of improvement and mitigation activities are reported to the Corporate Board and the IT Board of Deutsche Post DHL Group.

3.3 Operation of Information Security

Information is classified following a risk assessment approach and protected according to its classification.

Controls that mitigate risks are implemented in a timely manner and monitored to ensure their ongoing functioning and to support continuous improvement.

Information required to ensure the proper functioning of the Information Security Management System are collected, analyzed in a timely manner, and reacted upon appropriately.

Changes to the Information Security Management System and subsequent documentation are identified and monitored to manage the required level of Information Security. These changes are recorded, analyzed, reviewed, and approved by the appropriate level of management and documented according to a standard process.

Information Security events and incidents are treated appropriately by experts across Deutsche Post DHL Group.

3.4 Continuous Improvement of Information Security

Following Deutsche Post DHL Group's approach for continuous improvement, the Information Security Management System and subsequent documentation are reviewed annually and if required updated by the Information Security Committee.

The review takes into account significant changes to the external and internal context, the strategy of Deutsche Post DHL Group, and the results of relevant measurement and monitoring across Deutsche Post DHL Group.

4 DOCUMENT ATTRIBUTES

Document Owner	Authorizing Body	Date of Authorization	Current Authorized Version	Frequency of Review	Date of Last Review
Information Security Committee	IT Board	25 July 2013	1.0	n/a	n/a
Information Security Committee	Information Security Committee	22 February 2018	1.31	n/a	n/a
Information Security Committee	Information Security Committee	16 March 2020	2.00	Bi-Annually	n/a
Information Security Committee	IT Board	24 March 2020	2.00	Bi-Annually	n/a
Information Security Committee	Corporate Board	21 July 2020	2.00	Bi-Annually	n/a
DPDHL Group CISO	Information Security Committee	19 January 2021	2.01	Latest every two years	n/a
DPDHL Group CISO	Information Security Committee	19 January 2021	2-2021 Autumn	Bi-annually	14 September 2021
DPDHL Group CISO	IT Board	12 April 2022	2 – Spring 2022	Bi-Annually	12 April 2022

Deutsche Post AG

dpdhl.com

Effective from 5 October 2021