WHITEPAPER

LABFORWARD’S IT SECURITY POLICY

YANNICK SKOP

TABLE OF CONTENTS

INTRODUCTION

At Labforward, data protection and IT security have been our priority since the beginning. We are committed to implementing best-in-class information security measures and we also consider this to be an essential aspect of our business. We've established a Quality Management System (QMS) under ISO 9001 requirements (certified since 2021), and are currently pursuing an additional Information Security Management System (ISMS) certification under ISO 27001. By pursuing this additional certification, we are strengthening our internal information security controls and processes.

In this whitepaper, we summarize the most important IT security measures that are in place. For more information, a full, internal version of our IT Security Policy document (POL-002) is also available upon customer request.

LABFORWARD'S IT SECURITY POLICY

Our IT Security Policy document outlines the information security procedures and processes that apply to Labforward employees and contractors and is a critical part of Labforward's QMS and ISMS. This document serves to protect the confidentiality, integrity, and availability of the company's data as well as the data of its customers. This policy was established and is maintained and distributed by our Information Security Leadership Team, together with our Quality & Compliance Team. All Labforward employees and contractors are responsible for understanding and adhering to these policies, following the procedures outlined therein, and immediately reporting suspected or actual information security breaches.

IMPORTANCE OF IT SECURITY

Our Chief Technology Officer, Mario Russo, explains Labforward's commitment to Information Security:

"As a company which relies heavily on technology to collect, store, and process sensitive information, we are potentially vulnerable to information security breaches that may have significant adverse effects on our customers, our employees, our finances, and our reputation. In order to protect and secure this information and the trust placed in us by our board, investors, fellow employees, and customers, we prioritize information security to the highest degree and provide the necessary resources to develop,

implement, and continually improve our information security management practices."

In other words, the intention of Labforward's information security measures protects sensitive information that is entrusted to us. Through the implementation of an information security management system (ISMS), we can:

> Assure that we are satisfying all of our legal, regulatory, and contractual obligations.

> Ensure right-of-access to sensitive data only to the right people at the right time.

> Protect personal data, as defined by the GDPR.

> Be good custodians of all data we possess.

OVERVIEW OF LABFORWARD'S SECURITY PRACTICES

Labforward's Information Security Policy establishes and documents many important security practices, which our employees must be trained on and adhere to in all of their processes. These include:

1. Obligation to report suspected information security risks to the Information Security Leadership Team.
2. Adherence to regulations on whether, and how various devices may be utilized for work-related activities.
3. Guidelines on how to protect devices that are used to access company accounts or systems.
4. Mandatory installation of company-selected antivirus and password management software.
5. Course-of-Action to follow in the event of a missing or stolen device.
6. Conditions that must be met for our employees to work remotely effectively and securely.
7. A strict policy for appropriately unique, complex, long, and confidential passwords, in part generated and implemented by the company's password management software.
8. Usage of Single-Sign-On (SSO), two-factor authentication (2FA), and hard drive encryption mechanisms to protect our employees' user accounts and data.
9. Best practices to avoid scams, phishing prevention training, and training to identify and avoid malicious software distributed via email or suspicious links.
10. Rules for safe handling of information

transfer and file sharing, including how to handle removable storage media devices.

11. Maintaining a clean desk and clear screen policy to ensure that confidential materials are never viewable or accessible to unauthorized people.
12. Guidelines on how to use and protect shared facilities and equipment.

ENSURING EFFECTIVE IT SECURITY IMPLEMENTATION

Even the most solid IT Security Policy is worth very little if it is not adhered to by its target audience. To ensure the effective adoption of this policy, Labforward has implemented the following steps:

1. Mandatory employee and contractor training on the information security policies, concepts, and processes at Labforward.
2. Internal audits by the Quality & Compliance team, in addition to external audits, to monitor compliance with the IT Security Policy and related procedures.
3. Recording of corrective and preventive actions related to Information Security in our CAPA tracking system.
4. Regular risk assessment by the Information Security Leadership Team, as well as reviews by Labforward's Management Team.
5. Certification and recertification of our QMS and ISMS under the latest ISO 9001 and ISO 27001 standards.

CONCLUSION

At Labforward, we believe that we can only succeed in becoming a world-leading laboratory software company by protecting our customers' data. We will spare no effort to ensure that we:

1. Consistently meet or exceed our customers' expectations concerning excellence in informa-tion security.
2. Respond to challenges by immediate and decisive action, thereby improving our service delivery, company resilience, and customer satisfaction.
3. Identify, report, investigate, and resolve all instances of non-conformance and take action that prevents recurrence.
4. Continuously evaluate our internal Quality Management and Information Security Management Systems, including our information security processes and policies. Furthermore, ensure widespread and constant adoption of

these processes and policies, to guarantee high quality of our products and services.

5. Foster excellence in IT Security as one of our core values by educating and training our people to continually improve their knowledge and awareness of all aspects of information security.
6. Uphold regulatory compliance including an ongoing review of statutory obligations, standards, and codes of practice that apply to our business. Uphold regulatory compliance, in part by maintaining an ongoing review of statutory obligations, standards, and codes of practice that are particularly applicable to our business.
7. Promote and maintain a company culture that supports all aforementioned objectives.

If you have any specific questions about how Labforward protects your data, please feel free to contact our dedicated email address: dataprotection@labforward.io

CLARIFICATION OF ACRONYMS

2FA (Two Factor Authentication)
A security management method which requires two forms of identification to access resources and data.

CAPA (Corrective and Preventive Action)
Measures taken to either eliminate the cause of nonconformity or address a potential cause for nonconformity before it occurs, respectively.

GDPR (General Data Protection Regulation)
A regulation in EU law on data protection and privacy that applies to the EU and the European Economic Area. GDPR is both an important component of the EU privacy law and Article 8 of the Charter of Fundamental Rights of the European Union.

ISMS (Information Security Management System)
A set of policies and procedures for systematically managing our sensitive data. The ISMS framework at Labforward is designed in compliance with ISO/IEC 27001 standards.

ISO (International Organization for Standardization)
Develops international standards to regulate a broad range of manufactured products and services.

QMS (Quality Management System)
A collection of procedures present in a business to ensure consistent satisfaction of customer requirements. The QMS at Labforward is designed with risk-prevention-based thinking as its core basis and building block, as well as being in alignment with ISO 9001:2015, as per the company's interpretation of the international standard.`

SSO (Single-Sign-On)
An authentication scheme that allows its users to access several related, independent, software systems through a single ID.