labfolder GmbH
Elsenstraße. 106, 12435 Berlin, Germany
+49 (0) 30 86459390 | www.labfolder.com

Contact| labfolder Team
contact@labfolder.com
+49 030 / 91572642

Whitepaper:

labfolder Security

TABLE OF CONTENT:

INTRODUCTION 3

STATE-OF-THE-ART ENTERPRISE SECURITY 3

CONFIDENTIALITY 4

AUTHENTICITY 4

INTEGRITY 4

Introduction

Security is a key component of cloud computing and online services, such as digital lab notebooks and electronic archive facilities that deal with digital storage and online data processing. In particular online services used for research purposes need to implement strong and reliable security features that provide maximum protection for raw data, ensuring data quality and integrity of intellectual property.

Various methods of keeping data confidential and secure have highlighted not only questions about data ownership and maximum protection, but also how various vendors of cloud computing technologies build and implement their services. As a provider of reliable cloud services, labfolder incorporates security implications of the latest cloud computing model. These services, characterized by redundant computing environments, multiple state-of-the-art enterprise security features and emergency resource allocation, enable customers to access, share and manage their data - anytime and anywhere from all mobile devices.

labfolder's carefully developed state-of-the-art enterprise security consists of a combination of standard cryptography and real end-to-end encryption, a highly available hosted service and a safe and reliant infrastructure for maximum data security. Thus the labfolder system addresses all defining areas that ensure data quality and maximum intellectual property protection: confidentiality, authenticity and integrity.

This whitepaper at hand contains an overview of the implemented security features that allow labfolder to provide maximum data security for all customer data. labfolder can only provide a secure environment for all data stored in the electronic archives/labfolder system. However, this document does not give in-depth information on general data security, nor does it provide legal advice for full compliance. For other security measures, for example hardware components like mobile devices, the security regulations of the respected provider apply.

State-of-the-art enterprise security

labfolder incorporates state-of-the-art enterprise security - both logical and physical/environmental - to provide maximum protection for sensitive research data. labfolder's security program is based on a multi-layered security strategy that offers controls at multiple levels of data access, storage and transfer. The strategy includes the following components:

Operational security: Malware prevention program including security monitoring program and operating system security; network security with strict network firewalls and system access only allowed for verified IP addresses

Physical and environmental security: Secure data centre (TÜV approved data security and ISO 27001 certificate for excellent data security) with regular stress testing of infrastructure, climate protection procedures (e.g fire. water or other natural disasters), the provision of redundancies and emergency management

Access control: Authentication controls with a unique User ID, authorization controls with various access rights and levels and password complexity requirements

System development and maintenance: System check-ups with scanning and monitoring routines, regular security and functionality updates

Disaster recovery and business continuity: Validation plan and continuity and disaster recovery procedures

Regulatory compliance: Compliance with GxP Principles by by the Organisation for Economic Co-operation and Development (OECD) and the 21 CFR Part 11 of the Code of Federal Regulations

Corporate security policies: Specific security policies that cover physical, account, data, corporate services, network and computer systems, applications services, systems services, change management, incident response, and data center security. Regular review and updates to help ensure their continued e!ectiveness and accuracy.

Organizational security: Special procedure to maintain labfolder's defense systems with regular security review processes, including a customized security infrastructure and compliance to established security policies and standards. monitoring of routine security evaluations

Personnel security: All persons employed by labfolder must comply to labfolder's security policies. Employees are also given an educational security training on complying with labfolder's security policies, including the secure guidance of sensitive data, safe use of development software and secure programming.

Secure session management: Encrypted credentials and session-ID free URLs, multiple encryption, including encrypted passwords via salts cryptography, storage encryption, encrypted communication and encryption during uploads and downloads

Confidentiality

In order to keep all raw data confidential, restricted access management for authorized users only apply. The labfolder system addresses the confindentiality agreement by employing procedures that keep all data protected from disclosure to unauthorized parties, including:

Admission control: Limited access to data only for account owner and authorised persons

Data encryption: Encryption for identifiable data during uploads/downloads, transfer and storage

Secure storage: Separate security locations on redundant servers with various security procedures in place (both physical and logical)

Safe disposal: After confirmed deletion of an item, the data in question is removed and no longer accessible from that user's interface, labfolder's active servers and replication servers. Dereferenced data will be overwritten with other customer data over time

Confidentiality agreement: Records Management Section for staff working with sensitive research data, well trained personnel and internal security training

Authenticity

In order to access, manage and share experimental data, the identity of the user has to be verified. labfolder implements various functions that address the authenicity requirement, all guaranteeing the reliability of data management, transfers and exchange within research networks through:

Multi-level authentication processes: Login/password combination and access rights management

Secure user identification: Identification to access and to manage data

Electronic signatures: Sign and witness functions for digital data

Migration plan: Secure data transfer with encrypted coding and login/password combination

Integrity

In order to keep digital data in its original format (“intact”), labfolder employs several methods, assuring that the original remains unaltered during data transfer. The labfolder system provides comprehensive protection of research data from unauthorised access and changes through the following integrity features:

Access control: Restricted management rights to ensure data quality in a regulated environment

Authority checks: Limited access to authorized individuals only

Full audit trail: All activities within the system will be recorded

Version control. Recording and monitoring of all activities, including IT related processes

Logged data: Uploads and downloads are logged and “hashed” to verify data integrity

Timestamps: Records and changes are provided with a system-created timestamp, recording person, date and time

Electronic signatures: Option to sign and witness electronic documents

Secure data transfer: Migration plan with encrypted coding

Data retention: Long term retention of electronic records for at least 3 years until deleted by account owner

Data availability: Stored records are available for collection, inspection and review by the agency/reviewing body

Data deletion: Deletion of records can be controlled and prohibited by organizational policy

Standard Operation Procedures: SOPs to ensure optimal system performance and uninterrupted services, including validation, operation and maintenance

labfolder is committed to keep all data stored on its digital archiving facility system safe and secure. labfolder follows a strict and transparent policy to ensure the safety and security of valuable scientific data stored in the provided system. Each of labfolder’s multi-layered security strategy has been tested, endorsed and successfully implemented in the overall security program. labfolder values the privacy, confidentiality, integrity, and availability of customer data.

Contact:

Dr. Florian Hauer
labfolder GmbH
Elsenstraße 106, 12435 Berlin
Germany
Tel.: (+49) 30 / 91572642
e-mail: fh@labfolder.com