ICE
TRUSTED IT PARTNER

ICE's ULTIMATE GUIDE TO

EFFECTIVE LAB SECURITY POLICY

Trusted IT Partner SOC 2 Type II Certified

01
PURPOSE

This policy defines the baseline security for Life Science lab data when using any computer and communications systems dedicated to lab support operations. The purpose of this policy to is to provide a framework to support the lab environment security and safety. Any exceptions to this policy will be processed by the defined exception section below. Anything that is outside the scope of a desired exception to the rule can be submitted and reviewed.

Although all lab data is important, it should also be noted that several layers of security are included in the policy based on the type of data the Lab system uses or produces, i.e., PHI (Personal Health Information), PII (Personal Identifiable Information), or CUI (Controlled Unclassified Information) are considered controlled data, whereas normal test data and lab experiment data results are not considered controlled data. In this policy, differences in the type of data are noted as controlled lab systems or controlled lab data, and standard lab systems or data.

02
SCOPE

This policy applies to all lab users of its lab contractors, lab interns, and Lab systems vendors. This policy is to ensure the security and integrity of Your lab systems and that the data produced or used on the lab systems is maintained and protected.

03
BIOTECH LAB POLICY

INTERNET
Due to the sensitivity of the data produced or processed by the lab systems, all internet access is blocked on the Lab network via a firewall security policy by default.

INTRANET
To protect the proprietary data and lab results data from being compromised, all data into and out of the lab must be limited, protected, and controlled.

Intranet traffic, traffic between the different logical networks within your network, is restricted to connections from within the corporate network to the lab device or system.

A) Access to controlled lab devices (processing or producing controlled data) within the lab is restricted to whitelisted-only access and preferred through a jump host, proxy, or authenticated session to add an additional layer of security.

B) General Lab Devices can be accessed via a remote access session (such as RDP) from within the corporate environment.

From the Lab devices to any part of the corporate network, all traffic is blocked by default.

ELECTRONIC MESSAGING
Electronic Messaging (e-mail and chat) represents a high risk to your security of controlled and proprietary data, all access to electronic messaging is blocked from the Lab Systems.

If management allows personal phones or company issued devices (laptops and phones) in the lab area, email and chat services may be used on those devices on the corporate wireless or guest wireless network only, wired connections are not permitted to personal devices in the Lab.

ACCESS CONTROL TO LAB DEVICES
All lab systems are considered controlled or sensitive devices, and as such, access to these systems is controlled. Use of these systems is restricted to approved lab operations personnel and lab supervisors only.

Access by lab personnel, contractors, and interns

A) Active Directory Organizational Units (OU)s, security groups, or Access Control Lists (ACLs) will be utilized to control access to the lab systems.

B) Lab systems processing or producing controlled data will utilize multiple levels of access control (MFA) and the practice of least privilege will be utilized.

To protect the lab devices from possible exposure to risk, lab systems will not be placed on corporate Identity Management Systems (Active Directory, EMM (Endpoint Monitoring & Management), or MDM (Mobile Device Management) systems.

A) Since it is normal that several lab personnel will be accessing a single lab system, Authentication is important to identify the who and when the system is accessed, shared logins are not allowed.

B) Authentication should be through an identitymanagement system configured with the proper Access Control for the Lab personnel.

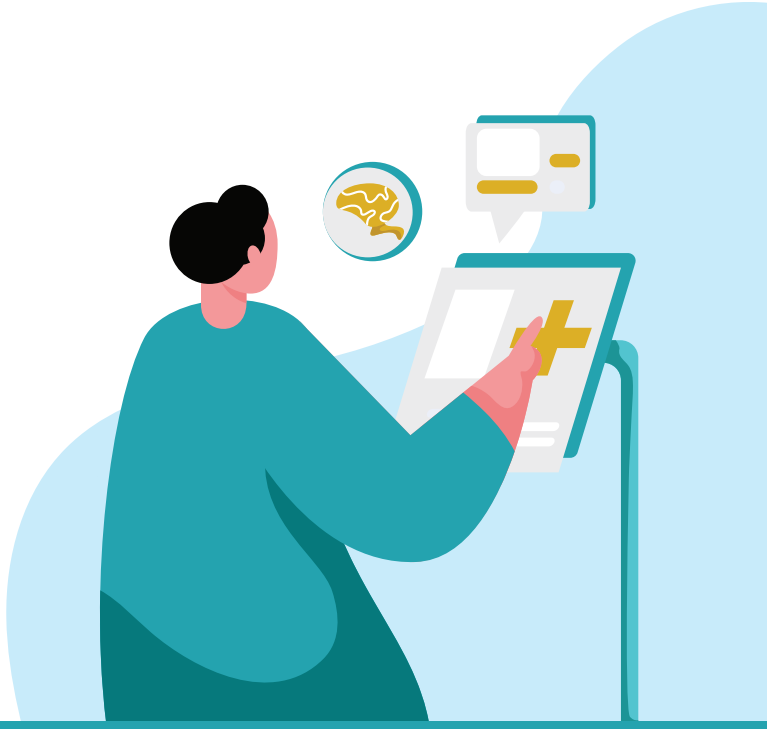
C) Additional requirements such as multi-factor authentication, Security tokens, or biometric authentication will be implemented on lab systems processing or producing controlled information.

Vetting of 3rd Parties and Vendors

All Lab Equipment and Systems must be vetted by the IT and Security Departments to validate the security posture of both the vendor and the lab system requirements before the purchase of Lab Systems is authorized by management. The vetting process includes checks for GRC (Governance, Regulatory, and Compliance), risk management, support, network connectivity, and data requirements. The use of unapproved or non-vetted vendors could jeopardize your proprietary and controlled data.

Review of Access Controls for Lab Devices

All access controls implemented will be reviewed by management on a quarterly basis to ensure that only approved access is granted to the appropriate personnel and vendors.



PHYSICAL SECURITY OF LAB SYSTEMS

General Lab physical security follows the standard "Two-Lock" principle, i.e., Badge Readers and the lab computer or device are physically secured. This might include placing it in a secure location or using a lockable cabinet, security cables, or cage to prevent unauthorized removal or access. Lab systems containing controlled data should have additional physical security measures implemented to protect the devices and the data, i.e., cameras, proximity alarms, two-man rule, etc.

INTERNAL SYSTEMS (BACKUPS AND IMAGES)

Your company has a designated data backup policy and solution for backing up corporate data, utilizing best practices on managed Air-Gapped solution with a backup routine approved by management. See the standard Data Backup and Retention Policy for details.

All Lab devices will be placed on a separate or isolated managed Air-Gapped backup solution and a three-tier backup routine (Daily, Weekly, Monthly) will be implemented to ensure Lab Data is captured and available in the event of a loss of data. This solution will be tested on a quarterly basis to ensure data can be restored in the event of loss of lab data.

Additionally, a complete system image of all lab systems will be copied on the Air-Gapped backup Solution at least monthly, and test restored on a quarterly basis.

EQUIPMENT FIRMWARE AND SOFTWARE UPGRADES

Standard Lab devices (attached to lab Instruments) without special software or application requirements will be upgraded to the latest approved security patch firmware or software versions once that release version has been verified by the vendor.

On certain lab systems, some Lab device vendors have specific system requirements and usually provide the data collection devices (i.e., a specially built laptop or desktop) with the Lab instrument. In these cases, the support, licensing, and upgrades for the lab devices are provided by the vendor.

SECURITY SOFTWARE INSTALLED ON LAB SYSTEMS

Experience with Lab devices has proven that common Managed Detection and Response (MDR), Extended Detection and Response (XDR), and Endpoint Detection and Response (EDR) security protection software may interfere with the proper operation of the applications and custom software designed for particular Lab instruments. As a result, MDR, XDR, or EDR software will be removed from common lab devices before deployment or connection to the lab instruments. This is a high-risk situation requiring this lab policy be strictly adhered to. Due to this, Lab devices are segmented away from other devices with your network to reduce the risk of infection and compromise. CIS Hardening of standard Lab Systems Operating Systems will be applied where possible.

SECURING INFORMATION (DATA STORAGE AND TRANSFER OF DATA)

Hard disk or whole system encryption security software will be installed on all lab systems to protect data stored in the device until transferred to a centralized data repository. No more than a couple of days or the current experiment's worth of data should be stored on the lab device, before transferring to a secure storage solution.

Lab results data and proprietary data will be stored on a management approved Data storage solution either on-premises or in a Private Cloud such as AWS, Azure, Enterprise DropBox, etc. The use of Onedrive or Gdrive should not used, as the risk is greater for data loss using repositories also containing regular corporate data.

All Lab systems should be set-up to write data to a secure data storage solution in an automated routine and stored encrypted to satisfy the "Encryption at Rest" guideline in common security frameworks (such as NIST 800-171, CIS framework, or Cobit guidelines).

When data is in transit, meaning the data is being moved from one location to another, the transit medium must also be secured and encrypted with approved encryption algorithms and security keys, "Encrypted in Transit".

REMOTE ACCESS TO LAB SYSTEMS

Access from Corporate networks

It is normal for lab personnel to access the Lab systems from the corporate network to monitor experiments, check the health of the devices, etc. during the normal course of their work. Remote Access to lab systems poses a security risk allowing a device from outside the lab to remotely access the system or the data. As such, a secure method of remotely accessing the lab systems will be approved by management and then implemented on a controlled basis utilizing the access controls mentioned earlier in this policy in accordance with the type of data the system being accessed processes or contains.

Remote Access of Lab Systems from outside your Company Network

Accessing Lab Systems from outside of your company Network by approved Lab personnel poses a higher risk of compromise than remote access from inside the network. Extra security controls such secure VPN connections, zero trust access, or encrypted tunneling will be implemented once approved by management and access reviewed on a Quarterly basis.

Lab System access by Vendor or 3rd Party

Certain Lab systems are required by the vendor and other 3rd Parties to be accessed remotely to monitor and check the health of the devices, upgrade applications and firmware, etc. Vendor Remote Access poses an extreme security risk allowing a device from outside the control of your network to remotely access lab devices containing proprietary and controlled data.

Remote control and monitoring of lab devices by a Vendor or other 3rd Party should be kept to a minimum and restricted to vetted and approved vendors only. Management must approve all remote access requests in writing for official records keeping.

An approved remote access solution will be installed on the Lab device and special security precautions such as specific time limit restrictions and special security policies on the Firewall will be implemented to isolate the affected lab devices from other lab devices and specific access control measures implemented, sometimes called “Micro-Segmentation”.

Requests for Remote Access to Lab Systems

All requests for Lab System Remote access must be forwarded to your IT and Security Departments in writing utilizing your request control system, i.e., Ticketing System. After approval has been received, a company approved remote access solution will be implemented.

All remote access solutions will be reviewed on a quarterly basis to ensure the company proprietary and controlled data are properly protected and risk management documents upgraded.

All 3rd Party Vendor access requests will also be forwarded to your IT and Security Departments in writing (Ticketing System) and in advance of the timeslot requested by the Vendor.

Since Vendor requests pose the highest risk to the containment of the Lab Data, each request will be reviewed separately and not just rubber stamped, what is the timeline the vendor is requesting, what type of data is being generated from the Lab system and would access disrupt the normal operations of the Lab device, etc. before approval can be given. Vendor access will be reviewed on a quarterly basis for continued relevance and requirements, and all expired or non-relevant access revoked.

04 REVIEWS

A formal review of all aspects of this policy will be reviewed at least annually. This review will be documented on the signature page of this policy document. In this era of ever-changing security threats and risks involved in the use of Lab systems, the review will include all policy sections for inclusion or deletion of certain aspects of the policy, new sections may be added at any time throughout the review period.

Certain sections of this policy have quarterly review controls and the review requirements are listed in those sections.

05 SUMMARY

A formal review of all aspects of this policy will be reviewed at least annually. This review will be documented on the signature page of this policy document. In this era of ever-changing security threats and risks involved in the use of Lab systems, the review will include all policy sections for inclusion or deletion of certain aspects of the policy, new sections may be added at any time throughout the review period.

Certain sections of this policy have quarterly review controls and the review requirements are listed in those sections.

06
DEFINITIONS

Confidential Information (Sensitive Information) – Any information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs, and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by a third party under a non-disclosure agreement.

Electronic Messaging System – Any device or application that will provide the capability of exchanging digital communication between two or more parties. Examples are electronic messaging, instant messaging, and text messaging.

Information Asset – Any company data in any form, and the equipment used to manage, process, or store company data, that is used while executing business. This includes but is not limited to corporate, customer, and partner data.

Objectionable Information or Material – Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes, and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected by national or international, federal, regional, provincial, state, or local laws.

Partner – Any non-employee who is contractually bound to provide some form of service to your company.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, to prevent unauthorized access to his account.

User - Any employee or partner who has been authorized to access any company's electronic information resource.