# Lab Security Standard

| | |
|---|---|
| **Standard Owner:** | Kevin Cross, CISO |
| **Responsible Domain Manager:** | Stephen Scaringella, Ed Hagopian |
| **Publication Date:** | January 5, 2021 |
| **Effective Date:** | January 5, 2021 |
| **Standard Location:** | SAFE@Dell P&S site |
| **Version No.** | 2.0 |

Related Policy: Information Security Policy

## Table of Contents

## 1 Purpose

The purpose of this Standard is to define the minimum security requirements that must be implemented and adhered to when building, managing, using and operating Dell Lab networks and systems. Unlike a data center used to house internal/corporate systems, a lab is a computing facility with controlled access used primarily for customer development, certification, testing, support and/or demonstrations. Labs can be physical, virtual, within a cloud service, in-house or at a co-located, or a combination of these alternatives.

Systems and resources hosted on the corporate networks/data centers are subject to the Dell security policies and standards listed on SAFE@Dell.

## 2 Scope

This Standard applies to team members of Dell Technologies and its subsidiaries ("Dell"), (unless the subsidiary has a separate and distinct policy or standard on the subject matter that is not in conflict with this Standard and contains statements that are as strict, or stricter than the terms set forth in this Standard), excluding SecureWorks and VMWare.

This Standard applies to all Dell employees, consultants, part-time and temporary workers, agents, vendors, and other independent contractors who perform work on or off Dell premises, at hosted or outsourced sites, or who have been granted access and are users of Dell information assets and supporting information technology resources or business processes. These individuals are collectively referred to as "Personnel".

## 3 Industry Standard Alignment

This Standard aligns with ISO 27001:2013, ISO 27002:2013, NIST SP 800-53 R4 and PCI DSS, as noted in the Industry Standard Mapping table in Section 7.

## 4 Definitions

A list of terms and definitions can be found in the Security and Resiliency Organization (SRO) Policies and Standards Glossary.

## 5 Roles and Responsibilities

| Role | Responsibilities |
|---|---|
| **Security and Resiliency Organization (SRO) - Cybersecurity** | Ensure all lab connections to Dell Technologies corporate firewalls and any Dell Technologies owned systems that support lab infrastructure environments are protected and secured. Provide baseline security configuration guidance. Approve internal and external network connectivity for Dell Labs. |
| **Dell Digital** | Manage and approve internal and external network connectivity for Dell Labs. |

| Role | Responsibilities |
|---|---|
| **Lab Management** | Ensure that the requirements of this Standard are implemented and maintained, for ensuring that sufficient resources and personnel are in place to meet these requirements, and ensuring their lab is listed in the Laso tool and that the Lab Manager, Lab network contacts and all other data fields are current and accurate.<br>Ensures that lab infrastructure is secured to the level outlined in this standard. Accountable for any physical third-party access to their lab. Audits, measures and reports on compliance with this standard. |
| **Lab Users and Guests** | Comply with the requirements outlined in this standard. |
| **Product Development** | Authorize access to source code. |

# 6 Standard Statements

1. All systems and networks designated for a Dell Lab environment must be deployed in accordance with this standard.
2. Lab networks must be subject to mutually agreed scheduled audits to assess and report on compliance to this standard, as well as applicable Dell Technologies policies and standards.
3. All Dell data stored or transmitted on Dell Lab networks and systems must be classified and appropriately protected in accordance with the Information Security Policy and the Information Security Governance Standard.
    a. No data or application governed by legal and/or regulatory requirements, including but not limited to Payment Card Industry (PCI), HIPAA, SOX, etc., must be stored in a lab environment or traverse a lab network.
    b. as "Restricted" or "Highly Restricted" created and stored on lab systems must be protected from unauthorized access and accidental loss in accordance with the Information Security Policy and the Information Security Governance Standard.
4. Intellectual property developed in Dell Labs is the property of Dell Technologies and must be protected as such.

## 6.1 Lab Inventory

1. An inventory of lab networks and subnets allocated to the lab must be established and maintained in an inventory tool that is accessible by Dell Digital and SRO-Cybersecurity approved tool, i.e., Lab Audit Survey Optimizer (LASO).
2. Lab network inventory information must be kept current and include, at a minimum:
    a. network name/subnet information;
    b. lab owner,
    c. lab manager; and
    d. lab network contacts.
3. All lab IP address space must be documented in the Dell IP address management (IPAM) tool and if further segmentation of this space is required, must be documented in a Dell Digital approved IPAM.

4. An inventory of all critical lab infrastructure assets must be established and maintained by Lab Management and made available to SRO-Cybersecurity and Dell Digital upon request.

## 6.2 Configuration Management

1. All software used in a Dell Lab environment must be legally licensed, including open source.
    a. All critical lab infrastructure (i.e., systems) that provide services to Lab Users, are hosted in the lab and necessary for lab operations, must be configured securely in accordance with SRO-Cybersecurity. Examples of such systems include:
        - WUS servers, File Servers;
        - build servers;
        - backup systems;
        - application systems (JIRA, Confluence, Qtest, etc.);
        - VM farms; and
        - network switches for distributing the lab network up to head of row switches
    b. Lab Management is responsible for developing and deploying standard configurations for systems.

## 6.3 Acceptable Use of Lab Systems and Networks

1. All personnel must be aware of their role in protecting Dell's information assets, supporting Dell's security and resiliency objectives and follow Dell's security policies and standards on SAFE@Dell at all times.
2. Lab Management must ensure that all Lab Users and Lab Guests are made aware of the Dell Technologies policies, standards and procedures pertinent to lab usage.
3. All activities performed in a Dell Lab environment or on a lab system must be for Dell approved business only and must be conducted in accordance with the Information Security Policy and Acceptable Use Policy.

## 6.4 Access to Lab Systems and Environment

1. Lab Management must establish processes and procedures for granting physical and logical access to Dell Lab environments for all types of access, users and guests.
    a. Third party remote access to lab resources necessary for emergency issue remediation must follow established emergency access procedures and must be authorized and approved by Lab Management.
        i. Emergency access must only be granted for a period of no more than two (2) weeks at a time and must be removed when no longer required.
        ii. Further extensions of the access must be approved by Lab Management.
    b. Any third party (i.e., non-Dell team member) user access must go through the Dell HR onboarding process before access to lab resources is granted.
    c. Lab Managers are accountable for any physical third-party access to their lab.

2. Access to Dell Lab systems, facilities, resources and source code, both physical or logical, must only be granted to users and guests with a legitimate need for access and must be authorized by the Lab Management.
    a. Access to Dell Lab systems, facilities, resources and source code must follow the principle of "least privilege" so that users are only assigned the rights they need to do their job and so that no user or guest has access to systems or source code that is not required for their role in accordance with the Access Management Standard.

## 6.5 Protection of Information and Source Code

1. Production business applications (i.e., Dell.com, quote and order information, Salesforce) and devices that store business application source code and data, or production business networking (e.g., PCI, Extranet, ICorp zones), must not be placed in a lab without SRO-Cybersecurity approval.
2. Source code that is created and stored on lab systems must be protected from unauthorized access and accidental loss and must be subject to the following security controls as a minimum:
    a. Source code must follow secure coding practices in accordance with the Secure Development Lifecycle (SDL) Standard.
    b. Source code must be backed up to code repositories that are hardened and secured in accordance with SRO-Cybersecurity configuration guidance.
    c. Backups of source code must be stored and protected from network-spread malware.
    d. Source code backups utilized for long term archival and disaster recovery must be encrypted at rest to protect sensitive information when stored.
    e. Audit trails for access, changes and deletions of data classified as "Restricted" or "Highly Restricted", must be recorded, maintained and protected from unauthorized access or alteration.
    f. Access to source code repositories must be restricted to personnel as authorized by Product Development.
3. The artifacts and binary files produced as an output of production product build processes on lab systems must be protected to maintain their authenticity and integrity as follows:
    a. Product binaries, which are to be distributed to customers as either software or firmware, must be digitally signed to provide customers with a means to validate their authenticity and integrity to maintain customer trust in Dell products.
    b. All product code signing operations must be performed using approved code signing infrastructure and processes as authorized by SRO Product and Application Security (PAS), which at a minimum must conform to the following requirements:
        i. The origin, authenticity and integrity of production code signing material used to sign final release builds must be verified and maintained to ensure that only approved production code signing material is provisioned into the code signing infrastructure and used to sign final release builds of product binary code.

ii. The infrastructure which facilitates storage and use of production code signing material must be secured in accordance with the Dell Technologies Policies and Standards and must be tightly controlled and audited to protect the confidentiality and integrity of production code signing material.

iii. Systems that access code signing infrastructure to sign final release builds must be protected with appropriate security controls as defined in the Dell Technologies Policies and Standards, and any additional controls defined in this standard to reduce the risk of compromise of the code signing process.

## 6.6 Patch and Vulnerability Management

1. Antivirus versions and signature files for critical lab infrastructure must be applied and maintained on all systems where available in accordance with the Endpoint Security Standard.
2. Lab infrastructure must be scanned monthly at a minimum for known vulnerabilities.
    a. Target remediation times for identified vulnerabilities, as defined in the Security Patch and Vulnerability Management Standard, must be observed.
    b. Exceptions require business justification and must be approved by Lab Management in addition to being approved with a Policy and Standard Exception (PSE).
3. Security patches must be applied to all critical lab infrastructure, at least quarterly. Security patches with a "Critical" and "High" score that are assessed and determined to be applicable must be applied within 30 days of release for systems containing "Highly Restricted" information and for high value assets (HVAs) and systems hosting critical infrastructure/ applications.
    a. Systems under test/development should apply best efforts to patch these systems when feasible.
4. Critical or production lab infrastructure systems in the DMZ must be fully patched as defined in the Security Patch and Vulnerability Management Standard.
5. Unnecessary packages, OS components and services that are not critical for testing or running the lab must be disabled or uninstalled on the lab infrastructure. Network connectivity to OSs with known security vulnerabilities must not be permitted unless authorized by the Lab Management.
6. Lab Management is responsible for the security and maintenance of the networks, VLANs and systems that reside within the lab environments. SRO-Cybersecurity will provide the necessary tools and execute these security scans within lab environments.
    a. Lab Management and any identified stakeholders must ensure that remediation activities and processes are followed in accordance with the Security Patch and Vulnerability Management Standard.
    b. All vulnerabilities identified as urgent/critical must follow the High Profile Vulnerability Process.
7. A list of all lab networks, DMZs and subnets must be maintained by Lab Management and made available to SRO-Cybersecurity.
8. Lab Management must establish and maintain formal incident management and notification procedures for any actual or suspected security incident occurring within

the lab environments. At a minimum, the procedures must include immediate notification of any suspected incident to SRO-Cybersecurity.

9. Where possible, all critical lab infrastructure systems must run an OS-based firewall utilizing least privilege. Lab Management must approve exceptions to this process.

## 6.7 Network Security

1. All Dell lab networks, whether hosted on-premise or in the cloud, or at a third party must be established and secured in accordance with the Network Security Standard.
2. A lab network may be either corporate routable or non-corporate routable:
    - Corporate routable lab networks are capable of reaching assets outside of that individual lab, including the Internet, limited corporate resources, and other labs not co-located.
    - Non-corporate routable must not route beyond their local corporate firewall. Cannot have direct access to Dell internal networks from the non-routable network.
3. Lab networks must be segmented from the Dell Technologies Corporate network by SRO-Cybersecurity managed firewalls.
4. Lab "Red" networks and "Core Blue" networks can co-exist in the same physical proximity, but physical and/or logical controls must be in place to prevent misuse.
5. Dell Lab cloud environments created outside of Dell need to ensure the network interface to and from the cloud are hardened in accordance with SRO-Cybersecurity guidance.
6. Network connectivity to/from labs via a corporate firewall must be limited to enable known legitimate traffic (including security monitoring/scanning tools) and block all other traffic.
7. Internet or other external/third-party network connections must be protected with firewalls managed by the SRO-Cybersecurity.
8. Labs containing systems that cannot comply with hardening, patching and access control standards must not have direct outbound internet access and must be segmented from other lab resources.
9. Labs that contain HVAs (e.g., Tier 1 source code) must follow controls defined in the Secure Development Lifecycle (SDL) Standard.
10. Lab network configuration changes that affect the lab's security posture must be reviewed and approved by Lab Management and shared with SRO-Cybersecurity.
11. Lab networks must be subject to penetration testing by SRO-Cybersecurity on a frequency commensurate with the risk and in consultation with the Lab Management.
12. Lab Internet connections must be owned, controlled and secured by Dell Technologies, SRO-Cybersecurity and Dell Digital.
13. Lab Internet connections must have appropriate security controls in place, including firewalls and intrusion prevention systems (IPS) in accordance with the Endpoint Security Standard.
14. Lab Internet access must be designed and deployed based on Dell Digital and SRO-Cybersecurity approved network designs.

15. Where remote access to Lab networks is required, VPN connectivity must be used in accordance with the Network Security Standard and Remote Access Standard.
16. Lab Management must review all lab assets that require access to corporate resources and must be approved by SRO-Cybersecurity.
17. All hosts in a lab environment that communicate directly with hosts in the Corporate security zone must communicate through a DMZ in the corporate security zone and must have corporate routable IP addresses. NATing between zones requires Lab Management review and SRO-Cybersecurity approval.
18. Lab DNS servers must log locally and retain logs for a minimum of 90 days or send their recursive query logs to the SRO-Cybersecurity Splunk instance.
19. Tunneling protocols, SSH, and ports related to AD and file sharing require Lab Management's review and SRO-Cybersecurity approval.
20. Lab to lab network interconnectivity via WAN must be designed and built as a joint effort between Lab Management and Dell Digital and then approved by SRO-Cybersecurity.
21. Dual-homing systems or other workarounds to enable traffic between lab and corporate (or crossing any segmented security zones), including wireless, is prohibited.
22. Users connecting to labs through any Lab remote access solution must not have unrestricted access to other security zones, including the corporate network. Remote access will only be permitted over certain authorized ports on the Lab-to-Corporate firewalls as approved by SRO-Cybersecurity. Users needing full connectivity to the Dell Technologies corporate network and other security zones (besides the lab) must use the Dell Technologies corporate VPN solution with Dell Digital owned assets.
23. For Corporate Dell Digital and SRO-Cybersecurity approved VPN clients, "Client Posturing" and Two Factor Authentication (2FA) are required for remote connectivity to lab networks.
24. Remote users must be automatically disconnected from the lab network after 12 hours of inactivity, requiring users to re-login to reconnect to the network. Pings, reverse tunnels or other artificial network processes are not to be used to keep the connection open.
25. Only Lab Management approved systems may be connected to lab networks.
26. Lab Management must request a global network address space from the Global Network Telecommunications (GNT) team and follow IP addressing procedures.
27. Lab Wireless LAN implementations are the Lab Network Managers' responsibility that controls the space they operate. Lab Management must ensure that all wireless implementations active in their space follow the standards defined in this Standard and procedures. Lab Management must approve exceptions to this process.

### 6.7.1 Wireless Access

1. All wireless access points must be securely configured so that they are inaccessible to unauthorized personnel.
2. Wireless communication networks must be consistent with applicable laws and regulations.

3. Lab Managers are responsible for updating software, hardware and firmware of wireless devices to ensure that vulnerabilities are addressed.
4. The use of WAP, WEP, OPEN, and other weaker security methods is not permitted.
5. If there are lab wireless access points (WAPs) that do not have owners and conform to the above standards, those WAPs/networks will be classified as "Rogue" and must be disabled and removed.
6. Lab Management is required to follow these standards and avoid interference with the CORP wireless network. If any deviation from these standards is required due to a valid business case, Lab Management must obtain approval from Dell Digital and SRO-Cybersecurity.

## 6.8 Authentication and Access Controls

1. SRO- Cybersecurity must approve authentication and authorization solutions between lab networks and corporate networks.
2. Labs are subject to all the requirements in Access Management Standard, which relate to provisioning (requesting, approving, granting, terminating), auditing, and/or reviewing access. Key requirements of this Standard include:
    a. a record of access requests and approvals must be retained by the personnel responsible for approving access;
    b. approval of the Lab Manager or the BU resource owner is required for access to resources within the lab, and
    c. new accounts must be assigned passwords that are then required to be changed upon first use.
3. Passwords must comply with the Password Standard (i.e., timeframe and complexity).
4. Test infrastructure and accounts used for testing and test automation must be only used on test environments, documented by the Lab Management and, where possible, stored in a key vault.
5. Test accounts can only exist in the non-critical infrastructure segments of the lab.
6. Authentication and logical access to lab network systems must be in place such that only approved employees and registered vendors/contractors can access lab networks and infrastructure.
7. HVA systems must only be accessible using corporate or lab identities.
8. Labs must use authentication systems and access control mechanisms such as Corporate Dell Digital Managed Active Directory for systems that contain Dell confidential information, as approved by SRO-Cybersecurity.
9. Where lab-specific authentication systems like Active Directory, identity stores and access control mechanisms are used, Lab Managers or BU resource owner is required to document the following:
    a. processes and records for the requesting, approving and provisioning user identities and access rights, and
    b. processes and records for regular review and termination of accounts.

10. Lab managers must have access to necessary credentials for all lab assets to enable timely patching of vulnerabilities (e.g., ISGADMIN account). Such credentials must be stored in a secure password vault as approved by SRO-Cybersecurity.

### 6.9 Special Lab Use Cases

1. Some labs, due to their use and nature, have special use cases that require specific considerations as described below.
    a. Manufacturing support labs can have special non-routable networks where the following allowances can exist. These network segments:
        i. Can use factory default usernames and passwords to test equipment and restore factory default settings to equipment prior to being shipped to a customer.
        ii. Can have systems with an unsupported OS or embedded systems in support of the customer or manufacturing effort.
        iii. Must still be scanned for vulnerabilities.
    b. Executive Briefing Centers (EBC) and Customer Solution Centers (CSC) spaces can temporarily (<30 days) deploy equipment and applications that are not approved by Technology and Architecture Global Standards (TAGS) for demonstration purposes only.
    c. Service Labs can have special non-routable networks where the following allowances can exist. These network segments:
        i. can have end-of-life systems in support of the customer;
        ii. can have end-of-life and unsupported embedded OS in support of the customer; and
        iii. must still be scanned for vulnerabilities.
    d. For PGNET:
        i. 2FA is not required for the VPN managed by the lab security team to access the PGNET lab network.
        ii. End-of-life system that are isolated from the rest of the lab and corporate networks are allowable.

## 7 Industry Standard Mapping

This Standard aligns with the following industry standards.

| Industry Standard Control | Authoritative Framework | Aligned Standard Statement |
|---|---|---|
| Isolate rogue devices after a rogue device has been detected. | NIST 800-53 r4 CM-8(3)(b) | 6.6.21 |
| Perform penetration tests, as necessary. | PCI DSS 11.3, 11.3.4 | 6.6.6 |
| Perform internal penetration tests, as necessary. | PCI DSS 11.3.2 | 6.6.6 |

| Industry Standard Control | Authoritative Framework | Aligned Standard Statement |
|---|---|---|
| Perform vulnerability scans, as necessary. | PCI DSS 11.2.1 | 6.5.2 |
| Perform internal vulnerability scans on the organization's systems. | PCI DSS 11.2, 11.2.3, 11.2.1<br>NIST 800-53 r4 RA-5a., RA-5b.1., RA-5b.2., RA-5b.3., RA-5(1) | 6.5.2 |
| Review the Access Control policies, as necessary. | NIST 800-53 r4 AC-1b.1 | 6.7.5, 6.7.7 |
| Control access rights to organizational assets. | ISO 27001:2013 A.9.2.3, A.9.4.1<br>ISO 27002:2013 § 9.2.3, § 9.4.1 | 6.7.2, 6.7.3, 6.7.4, 6.7.5 |
| Segregate servers that contain restricted data or restricted information from direct public access. | PCI DSS 1.3 | 6.6.1, 6.6.2 |
| Include restricting inbound internet traffic in the firewall and router configuration standard. | PCI DSS 1.2.1 | 6.6.3 |
| Include requirements for a firewall at each Internet connection and between any demilitarized zone and the internal network zone in the firewall and router configuration standard. | PCI DSS 1.1.4 | 6.6.2 |
| Control remote access through a network access control. | NIST 800-53 r4 AC-17(3) | 6.2.1, 6.6.10, 6.6.18 |
| Employ multi-factor authentication for remote access to the organization's network. | PCI DSS 8.3.2 | 6.7.4 |
| Maintain and review facility access lists of personnel who have been granted authorized entry to (and within) facilities that contain restricted data or restricted information. | NIST 800-53 r4 MA-5b., PE-2a., PE-2d. | 6.2.1, 6.2.2 |
| Include access control mechanisms in the Acceptable Use Policy. | PCI DSS 12.3.2 | 6.1.1, 6.1.2 |
| Establish and maintain an Incident Management program. | NIST 800-53 r4 IR-7(1) | 6.5.6 |
| Establish and maintain access rights to source code based upon least privilege. | ISO 27001:2013 A.9.4.5<br>ISO 27002:2013 § 9.4.5 | 6.1(4) |

## 8 Related Policies and Standards

Endpoint Security Standard

Access Management Standard

Information Security Governance Standard

Information Security Policy

Acceptable Use Policy

Network Security Standard

Password Standard

Secure Development Lifecycle (SDL) Standard

Security Patch and Vulnerability Management Standard

Remote Access Standard

## 9 Supporting Process, Procedures and Guidelines

Lab Audit Survey Optimizer (LASO) Tool

Lab Security site

Technology and Architecture Global Standards (TAGS)

## 10 Awareness and Training

Dell Technologies has adopted tools and training materials to assist you in properly managing Dell Technologies' information. Information and training modules are available on the Security and Resiliency Organization's Security Awareness & Training website.

## 11 Asking Questions

If any requirement in this document is unclear to you, please seek clarification before commencing with related activities by contacting Security@Dell.com.

## 12 Reporting and Investigations

It is imperative that you immediately report any suspected or actual violation of this Standard by a Dell Technologies employee or third party to your manager or Security@Dell.com. Anyone reporting a suspected or actual violation of this Standard in good faith is protected from retaliation under the Dell Technologies Code of Conduct. Any suspected unethical behavior that appears to violate the Dell Technologies Code of Conduct must be reported immediately to Ethics@Dell.com. All good faith allegations of violations of this Standard will be thoroughly and confidentially investigated. You are required to cooperate with all investigations of alleged Policy and Standard violations.

## 13 Discipline and Other Consequences

Employees who violate this standard are subject to appropriate disciplinary action or other remedial measures up to and including termination of employment if warranted under the circumstances and permissible under applicable law. Assigned workers and third parties who violate this Policy and Standard are subject to being denied access to Dell Technologies' facilities, personnel and assets and permission to perform services on Dell Technologies' behalf.

## 14 Administrative Guidelines

- This Standard may be revised or revoked by the Standard owner at any time, with no

notice.

- This Standard is a statement of intent only and does not create contractual rights. Dell Technologies reserves the right to make exceptions to this Standard at its discretion.
- This Standard is globally applicable unless contrary to local laws and regulations. Operations in different countries may have more stringent policies or implementing procedures where required by local law. In the event of a conflict, these more stringent local policies and implementing procedures will take precedence.
- Requests for exceptions to this Standard must go through the P&S Exception process.

## 15 Non-Disclosure

The information contained herein is proprietary to Dell Technologies and must not be disclosed to Non-Dell Technologies personnel unless bound by an NDA executed by Dell Technologies. The retention and use of this document constitute an agreement to protect the information contained within.

**Sharing of this document with Non-Dell Technologies team members and or third parties must have written approval from** Security@Dell.com.

## 16 Document History

| Date | Version | Description | Submitted By | Approved By |
|---|---|---|---|---|
| 05JAN21 | 2.0 | Annual review and update, removed Dan Grady as RDM. | SRO Governance, Risk and Compliance Julie Dennis Sherrie Smith | Kevin Cross |
| 24MAR20 | 1.3 | Updated PSE link | SRO Governance, Sherrie Smith | SRO Governance |
| 07JAN20 | 1.2 | Annual review, updated RDM | SRO Governance, Sherrie Smith | Kevin Cross |
| 27JAN19 | 1.1 | Updated Owner | SRO Governance, Angela Davis | SRO Governance |
| 28SEP18 | 1.0 | Dell/EMC Integrated Standard | Abhijit Kulkarni, Dave Albertson, Fred Bahrenburg, Joseph Cuteri | Michael Craigue, Interim CISO |