

HIWAY Principle:

Scope should be expressed as a list of assets

Assets

| Asset Types | CUI Relationships |
|-------------|---|
| People | People handle and safeguard CUI |
| Information | Information is CUI, and information is used in safeguarding processes |
| Technology | Technology stores, processes, transmits, and safeguards CUI |
| Facilities | Facilities store and safeguard CUI |

Asset Capabilities

| Objective | People | Technology | Facilities |
|---|--------|------------|------------|
| 3.8.7 the use of removable media on system components is controlled. | ✓ | ✓ | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | ✓ | ✓ | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | ✓ | ✓ | ✓ |

DEFCERT



Asset Capabilities

| Objective | People | Technology | Facilities |
|---|--------|------------|------------|
| 3.8.7 the use of removable media on system components is controlled. | ✓ | ✓ | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | ✓ | ✓ | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | ✓ | ✓ | ✓ |

DEFCERT



Asset Capabilities

| Objective | People | Technology | Facilities |
|---|--------|------------|------------|
| 3.8.7 the use of removable media on system components is controlled. | ✓ | ✓ | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | ✓ | ✓ | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | ✓ | ✓ | ✓ |

DEFCERT



Asset Capabilities

| Objective | People | Technology | Facilities |
|---|--------|------------|------------|
| 3.8.7 the use of removable media on system components is controlled. | ✓ | ✓ | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | ✓ | ✓ | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | ✓ | ✓ | ✓ |

DEF CERT



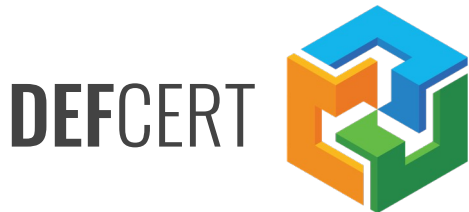
People Scope

Objective

3.8.7 the use of removable media on system components is controlled.

3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner.

3.8.9 the confidentiality of backup CUI is protected at storage locations.



People Scope

| Objective | Business Unit |
|---|------------------------|
| 3.8.7 the use of removable media on system components is controlled. | Defense Team |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | All employees |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Data Center Operations |

People Scope

| Objective | Business Unit | Role |
|---|------------------------|----------------------|
| 3.8.7 the use of removable media on system components is controlled. | Defense Team | System Administrator |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | All employees | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Data Center Operations | System Administrator |

People Scope

| Objective | Business Unit | Role | POC |
|---|------------------------|----------------------|---------|
| 3.8.7 the use of removable media on system components is controlled. | Defense Team | System Administrator | Carl J |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | All employees | - | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Data Center Operations | System Administrator | Ellen K |

DEFCERT



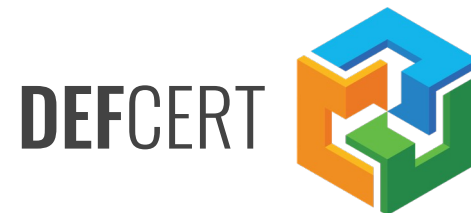
Technology Scope

Objective

3.8.7 the use of removable media on system components is controlled.

3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner.

3.8.9 the confidentiality of backup CUI is protected at storage locations.



Technology Scope

| Objective | Network | OS | Application |
|---|---------|----|-------------|
| 3.8.7 the use of removable media on system components is controlled. | | | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | | | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | | | |

Technology Scope

| Objective | Network | OS | Application |
|---|----------|----|-------------|
| 3.8.7 the use of removable media on system components is controlled. | - | | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Firewall | | |

Technology Scope

| Objective | Network | OS | Application |
|---|----------|----------------------|-------------|
| 3.8.7 the use of removable media on system components is controlled. | - | Windows, RHEL, macOS | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | Windows, RHEL, macOS | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Firewall | Windows, RHEL, macOS | |

Technology Scope

| Objective | Network | OS | Application |
|---|----------|----------------------|-------------|
| 3.8.7 the use of removable media on system components is controlled. | - | Windows, RHEL, macOS | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | Windows, RHEL, macOS | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Firewall | Windows, RHEL, macOS | - |

DEFCERT



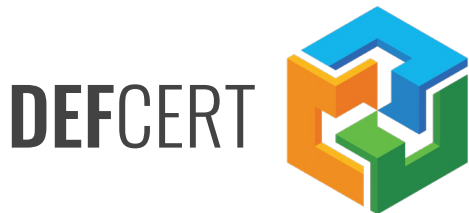
Facility Scope

Objective

3.8.7 the use of removable media on system components is controlled.

3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner.

3.8.9 the confidentiality of backup CUI is protected at storage locations.



Facility Scope

| Objective | Perimeter | Internal Zone | Rack/Enclosure |
|---|-------------|---------------|----------------|
| 3.8.7 the use of removable media on system components is controlled. | - | - | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | - | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Data Center | Server Room | Locked Rack |

DEF CERT



Facility Scope

| Objective | Perimeter | Internal Zone | Rack/Enclosure |
|---|-----------|---------------|----------------|
| 3.8.7 the use of removable media on system components is controlled. | - | - | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | - | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | - | Server Room | Locked Rack |

DEF CERT



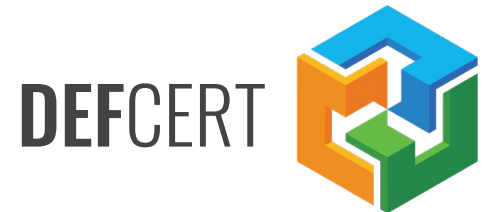
Facility Scope

| Objective | Perimeter | Internal Zone | Rack/Enclosure |
|---|-----------|---------------|----------------|
| 3.8.7 the use of removable media on system components is controlled. | - | - | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | - | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | - | - | Locked Rack |

DEFCERT



What about gaps?



Asset Capabilities

| Objective | People | Technology | Facilities |
|---|--------|------------|------------|
| 3.8.7 the use of removable media on system components is controlled. | ✓ | ✓ | |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | ✓ | ✓ | |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | ✓ | ✓ | ✓ |

DEFCERT



Technology Scope

| Objective | Network | OS | Application |
|---|----------|----------------------|-------------|
| 3.8.7 the use of removable media on system components is controlled. | - | Windows, RHEL, macOS | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | Windows, RHEL, macOS | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Firewall | Windows, RHEL, macOS | - |

DEFCERT



Technology Scope

| Objective | Network | OS | Application |
|---|----------|----------------------|-------------|
| 3.8.7 the use of removable media on system components is controlled. | - | - | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | - | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Firewall | Windows, RHEL, macOS | - |

Technology Scope

| Objective | Network | OS | Application |
|---|----------|----------------------|-------------|
| 3.8.7 the use of removable media on system components is controlled. | - | - | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | - | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Firewall | Windows, RHEL, macOS | - |

Technology Scope

| Objective | Network | OS | Application |
|---|----------|---------------------------|-------------|
| 3.8.7 the use of removable media on system components is controlled. | - | EDR – USB Allowlisting | - |
| 3.8.8 the use of portable storage devices is prohibited when such devices have no identifiable owner. | - | EDR – USB Allowlisting | - |
| 3.8.9 the confidentiality of backup CUI is protected at storage locations. | Firewall | Windows, RHEL, macOS | - |

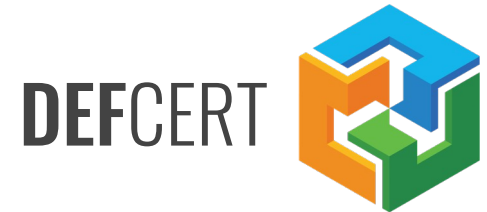
DEFCERT



Applicability Matrix

| Asset | Requirements |
|----------|---------------------|
| Firewall | 3.8.9 |
| Windows | 3.8.7, 3.8.8, 3.8.9 |
| RHEL | 3.8.7, 3.8.8, 3.8.9 |
| macOS | 3.8.7, 3.8.8, 3.8.9 |
| EDR | 3.8.7, 3.8.8 |

Notes on Applicability



Requirements Apply to Asset Type(s)

| Requirement | Asset | Asset Type |
|--|---|--|
| 3.7.6 Supervise the maintenance activities of personnel without required access authorization. | Personnel | People |
| 3.10.4 Maintain audit logs of physical access. | Audit logs | Information |
| 3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | Organizational systems Inbound communications traffic Outbound communications traffic | Technology Technology Technology |
| 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. | Facility Support infrastructure | Facility Facility |

DFC
CERT



Requirements are Limited by Conditions

| Requirement | Asset | Condition |
|---|--|------------------------------|
| 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms. | mobile devices mobile computing platforms | containing CUI |
| 3.4.9 Control and monitor user-installed software. | software | user-installed |
| 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. | privileged accounts non-privileged accounts | Nonlocal (network) access |

DEFCERT

