



Context and Purpose

The University has in excess of \$175m of research material stored in over 380 Controlled Environment Devices. Given the value of this investment and the inherent storage risks, it is essential that appropriate management practices are employed.

This procedure outlines a series of responsibilities and actions to ensure storage risks are mitigated in accordance with the Controlled Environments Policy.

Responsibility

The Deputy Vice Chancellor: Research and Enterprise is responsible for ensuring adherence to this Procedure.

End Users are responsible for ensuring that risks associated with storing their materials within Controlled Environments are appropriately mitigated.

Device Managers are responsible for ensuring that Controlled Environment Devices operate effectively.

Finance Unit is responsible for ensuring appropriate insurance cover is in place for Controlled Environments.

Procedure

A. Induction and Training

Prior to using a Controlled Environment Device, all End Users and Device Managers must undertake a tailored induction program, performed by the local area.

As part of the induction program, End Users and Device Managers must:

- be provided with a copy of the Controlled Environment Policy and Procedure
- complete relevant online training modules such as:
 - [Biological Safety](#)
 - [Plant and Equipment Safety](#)
 - [Liquid Nitrogen \(LN2\)](#)
 - [Basic FreezerPro Processes 1](#)
 - [Basic FreezerPro Processes 2](#)

End Users who store chemicals in Controlled Environments must also complete the online [Chemical Safety module](#) and must also have attended [Chemwatch Training](#).

The Deputy Vice Chancellor: Research and Enterprise will ensure annual audits are undertaken to assess compliance with Controlled Environments induction and training obligations. Corrective action will be taken as required.

B. Risk Assessment and Mitigation

All End Users must estimate the value of their materials stored within Controlled Environment Devices to determine the corresponding Importance Category and risk mitigation, as show in Table 1 below.

Table 1 – Importance Categories

1	2	3	4	5	6
Row 1 - Required Elements		Temp. detection alarm required	Back-up power required	Room access control	Emergency contact list
Value of contents to replace and/or cost of damage caused by overheating of stored chemicals	Importance Category				
\$500,000 +	CRITICAL	REMOTE Alarm	YES	YES	YES
\$100k <\$500k	VERY HIGH	REMOTE Alarm	YES	YES	YES
\$10k <\$100k	HIGH	REMOTE Alarm	YES	YES	YES
\$2k < \$10k	MEDIUM	LOCAL Alert	NO	Optional	Optional
\$500 < \$2k	LOW	NO	NO	Optional	NO
<\$500	NEGLIGIBLE	NO	NO	NO	NO

Information on how to value research material is available on the [Controlled Environment Devices SharePoint](#) site.

Where the Importance Category is assessed as High, Very High and Critical, material must be stored in high grade laboratory devices. Materials with an Importance Category of Medium, Low or Negligible may be stored in non-laboratory grade devices (i.e. commercial grade) if the device is assessed as fit for purpose. Devices manufactured for domestic purposes must not be used.

End Users must also consider the type of material being stored in Controlled Environment Devices and whether it presents a risk to health and safety. Ultimately, a holistic assessment of Controlled Environment Device risks must be undertaken.

Prior to purchasing a Controlled Environment Device, the Device Manager must complete a Pre-Purchase Checklist (Refer [WHS 79](#)).

Once a Controlled Environment Device is received, the Device Manager must also ensure:

- a Plant and Equipment Risk Assessment form is completed ([WHS 41](#))
- the Controlled Environment Device is entered in the University's enterprise system (FM:Interact)

FM:Interact is the University's definitive source of information relating to Controlled Environment Devices and Device Managers are responsible for maintaining the accuracy and currency of the information therein. Protocols for managing and maintaining Controlled Environment Devices are documented within the Controlled Environment Device Guideline.

The Facilities Management Unit will support Device Managers to ensure that risk mitigating infrastructure such as monitoring, alarm & security systems, and back-up power, is installed on Controlled Environment Devices in accordance with the Importance Category and Risk Assessment.

C. Inventory of Stored Materials

When a large number of samples will be stored for long periods of time (ie > 1 year), or genetically modified samples are stored for any length of time, End Users must ensure the stored material is catalogued within FreezerPro®.

Where a small number of materials will be stored for short-medium periods of time (ie < 1 year) End Users may catalogue the stored material within FreezerPro®.

Device Managers in conjunction with End Users must audit all stored material at least every 5 years. Materials that are no longer required should be disposed of to prevent proliferation of Controlled Environment Devices.

Where chemicals are stored, Device Managers must ensure the chemicals are recorded in the UniSA Chemical Manifest (Chemwatch®) and the appropriate hazardous symbols are displayed on the outside of the cold storage device in accordance with the Safe Management of Chemicals Procedure.

Device Managers must audit chemical storage in Controlled Environment Devices annually, ensuring that all devices are fit for purpose with all mitigation measures in place and operational (eg alarming and back-up power).

D. Device Maintenance

Regular maintenance is essential to prolong the life of Controlled Environment Devices and reduce the risk of potential failures.

Device Managers will establish a maintenance program for all Controlled Environment Devices, covering preventative and breakdown maintenance. At a minimum, maintenance programs should address legislative requirements and manufacturers' recommendations.

Device Managers will document the agreed maintenance program outlining:

- equipment to be maintained
- maintenance tasks to be undertaken
- frequency of maintenance
- person responsible for undertaking a maintenance task

Device Managers will ensure maintenance records are kept that document what was done, when and by whom.

E. Notifications and Alarms

The Facilities Management Unit will coordinate the monitoring of Controlled Environment Devices in accordance with parameters stipulated by End Users within FM:Interact.

If the monitored criteria move outside of the pre-set parameters, a notification will be sent via email from UniSA's Critical Equipment Monitoring System to the specified recipients.

If an alarm is triggered based on parameters set on the actual Controlled Environment Device, then a remote Security Monitoring Centre will contact the nominated alarm recipients (in order) on the mobile phone number(s) listed within FM:Interact.

The alarm recipient is responsible for taking initial corrective action to investigate the alarm and mitigate any potential loss of stored materials. Depending on the nature of the alarm / event, End Users and / or Device Managers may need to move the stored material to another device.

F. Device Relocation, Decommissioning and Disposal

If a Controlled Environment Device requires relocation, the Device Manager must:

- submit a [Customer Service Request](#)
- liaise with laboratory staff, relevant students and Finance Unit's Insurance office regarding the transfer of samples, as necessary
- transfer or remove inventory_swiftly
- Update the relevant information in FM:Interact to reflect the new parameters / location
- update material storage details in FreezerPro or ChemWatch_as required
- perform an End to End test

Disposing of any plant, including Controlled Environment Devices, may include reselling, in full or part, scrapping, waste disposal or recycling.

When disposing of Controlled Environment Devices, Device Mangers must:

- ensure that the device status is updated in FM:Interact
- remove the item from any other plant register, and
- complete an asset disposal form (FS64) as appropriate

Definitions

Controlled Environments: Any environment that requires a controlling mechanism / parameter to manage environmental conditions such as temperature, air pressure, air quality, humidity, lighting and water quality.

Controlled Environment Device: Any equipment, device, or facility that creates a controlled environment, including but not limited to refrigerators, freezers, cool rooms, dewars, fish tanks, greenhouses, herbaria and sterilised housing.

End Users are persons who store their material within a Controlled Environment.

FM:Interact is UniSA's enterprise space and asset management system, administered by the Facilities Management Unit.

Device Managers include all staff directly responsible for managing Controlled Environment Devices.

- **Associated Documentation**
 - [Controlled Environments Policy](#)
 - Controlled Environments Guideline
 - [Safe Management of Chemicals Procedure](#)
- **Officer Responsible for Update and Review:** Deputy Vice Chancellor: Research and Enterprise
- **Approving Authority:** Vice Chancellor
- **Commencement Date:** December 2022
- **Review Date:** December 2027
- **History:**.Nil