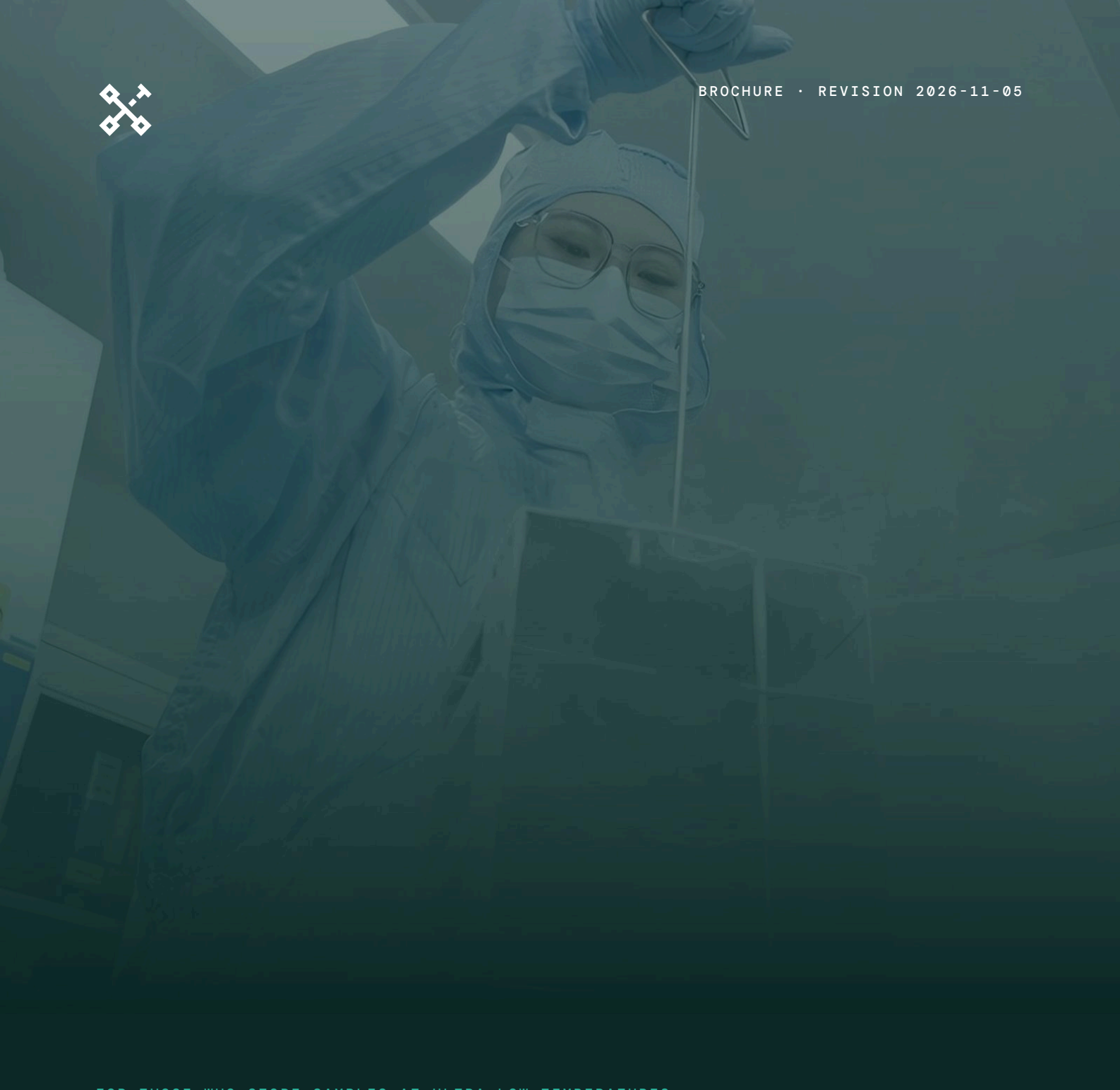


FOR THOSE WHO STORE SAMPLES AT ULTRA-LOW TEMPERATURES

Protect what cannot be replaced.

A handbook in basic cybersecurity for ultra-low freezers, liquid nitrogen tanks, cold rooms and their monitoring.

XERTIFIED AB · UPPSALA, SWEDEN

XERTIFIED.COM

Contents

Click a heading to go straight to the page.

01 **To those who store samples** — Page 3
Who this brochure is for and three things to do today

02 **The risks** — Page 4
The systems in the cold chain and how attackers usually succeed

03 **Checklist** — Page 5
Eight habits for secure storage

04 **Where do you stand today?** — Page 6
Take stock of your equipment and see where you stand

05 **Responsibility and rules** — Page 7
Who is responsible for what, and which rules apply

06 **Remote support** — Page 9
Questions to ask your vendors

07 **Freezers, tanks and alarms** — Page 10
Protect the freezers, the alarm chain and the network

08 **If something happens** — Page 11
What to do when a freezer alarms and whom to call

09 **Words and help** — Page 12
Words to know, more information and how Xertified can help

Only have five minutes? Start with Do this today on page 3.

Built on NCSC advice

This brochure follows the Swedish National Cyber Security Centre's (NCSC) in-depth advice on protecting OT environments (in Swedish). It also takes into account the regulations we describe at xertified.com/compliance. Thanks to NCSC for the guidance. NCSC has not reviewed this brochure.

The samples cannot be taken again

Eggs and embryos, a patient's own cells, biobank samples and unique seeds cannot be replaced. They are stored in ultra-low freezers at -80 °C and in liquid nitrogen tanks at temperatures down to -196 °C.

The freezers, nitrogen tanks and cold rooms are connected. They send alarms and data, often to the manufacturer's cloud service. Vendors reach them remotely for service. An attacker can use each of these ways in too.

This brochure helps you protect your storage. Most of it is about asking the right questions of the right people. Small steps make a big difference.

This brochure is written for

- hospital laboratories and IVF clinics
- biobanks, stem cell and tissue banks
- pharma and biotech, including cell and gene therapy
- clinical research organisations and central laboratories
- blood establishments and plasma companies
- universities and research infrastructure
- public authorities with laboratories
- wholesalers and cold chain logistics
- animal hospitals, veterinary labs and breeding
- gene banks for seeds and plants

DO THIS TODAY · THREE THINGS

1. **Test the alarm.** Run a test alarm and check that it reaches a person, also at night and at weekends.
2. **Ask who reaches the freezers remotely.** Ask the manufacturer, the monitoring vendor and the refrigeration contractor.
3. **Find out where the monitoring runs.** The server that sends the alarms should not sit on the same network as office computers.

The whole cold chain is connected

Storage depends on many systems connected to one or more networks. If the alarm is not active, no one notices the temperature rising.

Ultra-low freezers

Send data, often to the manufacturer's cloud service.

Nitrogen tanks

The controller fills nitrogen and raises alarms. Changed limits are noticed late.

Cold rooms and chillers

Often managed remotely by a contractor.

Monitoring

It sends the alarms. If it fails, they go silent.

Automated sample stores

The vendor reaches the store's computer remotely.

Oxygen monitors and access control

Protect staff and control who gets in.

How attackers usually succeed

- **Through a vendor.** The attacker gets into the vendor and uses its way in.
- **The equipment is visible on the internet.** Attackers search for it constantly.
- **Factory passwords are still in place.** Such passwords can often be found online.
- **Everything is on one network.** An attack on office computers reaches the monitoring.
- **The alarm is switched off** or runs over the same network that is under attack.
- **No one sees anything.** No one knows who changed a setting.

THIS HAS HAPPENED

- Attackers used a refrigeration supplier to change cold-room temperatures for blood plasma. The alarms caught it.
- A nitrogen tank's remote alarm was off when the tank failed. Thousands of eggs and embryos were lost.
- Ransomware knocked out a lab's IT for months. Thousands of hospital visits were postponed.

Eight habits for secure storage

Start here. Each habit makes life harder for an attacker and makes it easier for you to catch a fault in time.

01

Know what is connected

List the freezers, tanks, cold rooms, loggers and servers that are connected to the network.

02

Nothing reachable from the internet

Ask your vendors to check that no equipment can be reached directly from the internet.

03

Have an independent alarm

The alarm must work even if the freezer controller, the network or the power fails.

04

Test the alarm chain

Run a test alarm regularly. Check that someone responds and that no alarm is switched off.

05

Passwords and strong sign-in

Every device needs its own strong password. Remote access needs an authenticator app or a hardware key, not SMS.

06

Remote access only when needed

The vendor should only connect when there is a ticket, and only to its own equipment.

07

Divide and watch the network

Freezers, monitoring and cold rooms need separate network parts. Unknown traffic should raise an alarm.

08

Have a plan and practise it

Decide where the samples go and who moves them. Practise it, also without the network.

Tip: Go through the checklist with the lab, IT, medical engineering and facilities.

Take stock of your storage

Write down the equipment that is connected. Ask the vendor if you do not know the answer.

Equipment	Vendor and phone	Reachable from the internet?	Who reaches it remotely?
Ultra-low freezers			
Nitrogen tanks and filling			
Cold rooms and chillers			
Monitoring and loggers			
Alarms to on-call staff or alarm centre			
Automated sample store			
Oxygen monitors and ventilation			
Other:			

How secure is your storage?

Statement	Good	OK	Not yet
We know which equipment is connected.	☐	☐	☐
No equipment can be reached directly from the internet.	☐	☐	☐
The alarm works even if the network fails.	☐	☐	☐
We know which vendors have remote access.	☐	☐	☐
We know where the samples go if a freezer stops working.	☐	☐	☐

Start with what you ticked under Not yet.

Who is responsible for what?

The lab owns the samples. But the freezers, the network and the cold rooms may be run by IT, medical engineering, facilities or a vendor. Find out who is responsible for each part.

System	Lab	IT	Medical engineering	Facilities	Vendor
Ultra-low freezers	☐	☐	☐	☐	☐
Nitrogen tanks and nitrogen	☐	☐	☐	☐	☐
Cold rooms	☐	☐	☐	☐	☐
Monitoring and alarms	☐	☐	☐	☐	☐
The network	☐	☐	☐	☐	☐
Remote access	☐	☐	☐	☐	☐

> **Put it in the contract.** Agree who changes passwords, installs updates and closes remote access when a job is done.

Decisions that affect security

- Assume the equipment has vulnerabilities. It rarely gets security updates in time.
- Review the settings. Do not assume factory settings are secure.
- Keep logs long enough to investigate an incident afterwards.
- Write down every decision that lowers security, and why. Review these decisions regularly.

Rules to read more about

The table shows which regulations usually affect life sciences and laboratories.

A filled circle (●) means read this first. An open circle (○) means the rule may also affect you, for example through customers, suppliers or purchasing.

Regulation	Read	What it is
NIS2	● first	The EU directive on cybersecurity, applied through national law.
CER	● first	The EU directive on the resilience of essential services.
GMP and Annex 11	● first	EU rules for computerised systems in pharmaceutical manufacturing.
IEC 62443	○ also	The international standard for security in industrial systems.
ISO 27001	○ also	The standard for how an organisation manages information security.
NIST	○ also	US guidance on security, including for OT.
21 CFR Part 11	○ also	FDA rules for electronic records and signatures.

Specific to sample storage

- **National biobank laws.** In Sweden, for example, samples must be stored so that they are not at risk of being destroyed. Unauthorised persons must not get access to them.
- **The SoHO Regulation.** The EU's new rules for substances of human origin apply from 7 August 2027. They cover, for example, blood, plasma, tissues and cells.
- **GMP and 21 CFR Part 11.** In pharma, temperature data must be reliable and traceable.
- **NIS2.** Healthcare and pharmaceutical manufacturing may be in scope. NIS2 also sets requirements for the security of suppliers.

Which rules apply to you depends on factors such as size, services and customers. This is our reading, not legal advice. See the table for all industries.

Vendors that reach your equipment remotely

The freezer manufacturer, the monitoring vendor and the refrigeration contractor often need to reach their equipment. That speeds up service. But an attacker can use every way in too, sometimes through the vendor.

Questions to ask your vendors

1. How do you reach our equipment? Through a cloud service, an open port, a shared account or a secure connection?
2. What data is sent to your cloud service, and who at your company can see it?
3. Can you change settings or alarm limits remotely?
4. Does every technician have their own login, with an authenticator app or a hardware key?
    - Do you give logins to your subcontractors? If so, does every person there have their own login?
5. Can we approve each connection before it opens?
6. Can you show who connected, when and what was changed?
7. For how long will the equipment receive security updates?

Good answers

- We only connect when you have a ticket.
- Every technician has their own login, also at our subcontractors.
- We only reach our own equipment.

Warning signs

- The freezer has an open port. It has always worked.
- All technicians use the same password.
- We can change everything remotely.
- We don't know.

Read about secure remote access without open ports

Protect freezers and alarms

Freezers and cold rooms

The controller holds the temperature and sends alarms. A changed setpoint should show at once.

Nitrogen tanks

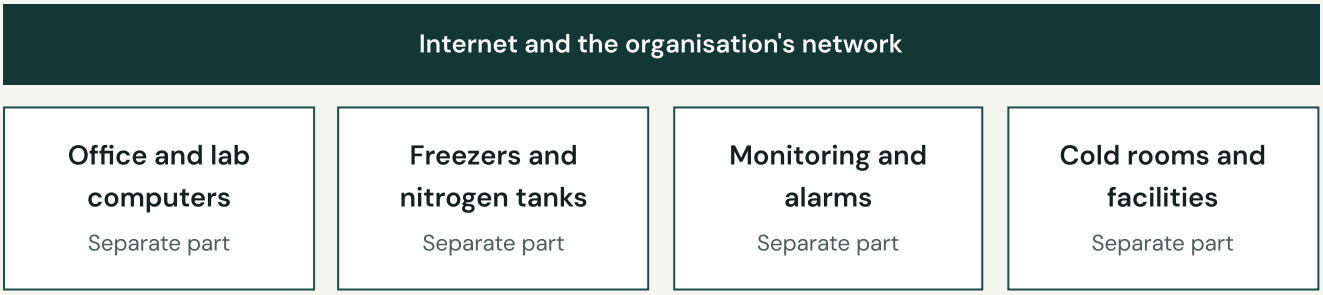
Fill status is the earliest warning. Check the alarm limits after every service visit.

Monitoring

Have an alarm that works even if the freezer, the network or the server stops working.

Divide the network

If everything is on one network, an attack on office computers can reach the monitoring. So divide the equipment into separate parts. Each part reaches only what it needs. Read about dividing the network



What to do

- Make sure no equipment can be reached directly from the internet.
- Let the freezer reach only the manufacturer's cloud service and nothing else.
- Send alarms two ways, for example over the network and over the mobile network.
- Protect the monitoring server against malware. Let it only raise alarms at first.
- Make sure alarms reach someone around the clock, also at weekends.

VALIDATED EQUIPMENT?

Equipment in a validated process is rarely changed. Protection in front of it does not have to change anything in it.

THINK ABOUT IT

If someone takes over the monitoring server, who notices that a freezer is warming up?

When a freezer alarms

1. **Save the samples first.** Follow your plan and move the samples to a freezer or tank that works.
2. **Check the temperature on site** with a thermometer that is not on the network.
3. **Find out what is affected.** One freezer, a cold room, the alarm or the whole monitoring system?
4. **Call the vendor's on-call service.** Tell them what you see and when it started.
5. **Close remote access** together with the vendor until you know what has happened.
6. **Document.** Write down what happened, when, which samples were affected and what you did. Follow your deviation procedure.
7. **Report the attack to the police.**
8. **Report the incident** to your national CSIRT. Also follow the reporting rules that apply to your organisation.

Prepare now

Fill in the list and put it up where staff can see it.

Contact	Name	Phone
Freezer vendor's on-call service		
Monitoring vendor		
Refrigeration contractor		
Nitrogen supplier		
IT on call		
Facilities on call		
Person responsible for the samples		

Words to know

Ultra-low freezer	A freezer that holds about -80 °C. Also called a ULT freezer or a -80 freezer.
Nitrogen tank	A tank that keeps samples cold with liquid nitrogen, down to -196 °C.
Alarm chain	The path from the sensor in the freezer to a person who acts.
Hardware key	A small device for signing in, such as a YubiKey. You plug it in or hold it against the computer.
Open port	An opening in the firewall that lets traffic in from the internet.
Factory password	The password the equipment has on delivery. It can often be found online.
Ransomware	Malicious code that locks computers and data and demands a ransom.
Validation	A check that shows the equipment works as intended. Every change may need a new check.

More information

CSIRTs Network	The national CSIRTs in the EU, from ENISA.
cert.se	CERT-SE, Sweden's national CSIRT.
NCSC on OT	The Swedish National Cyber Security Centre: in-depth advice on protecting OT (in Swedish).

How Xertified can help

We put a Lock in front of freezers, nitrogen tanks, loggers and the monitoring server. The equipment is invisible to unauthorised users and reaches only what it needs. XoT-Clients can sign in with a YubiKey or a smart card.

The vendor gets access to the right equipment for a set time. You can approve each connection and see who was in. The equipment is not changed. XoT does not measure temperature and does not replace your alarm.

xertified.com/industries/life-science · info@xertified.com · +46 18 265 06 06

Book a meeting or a demo