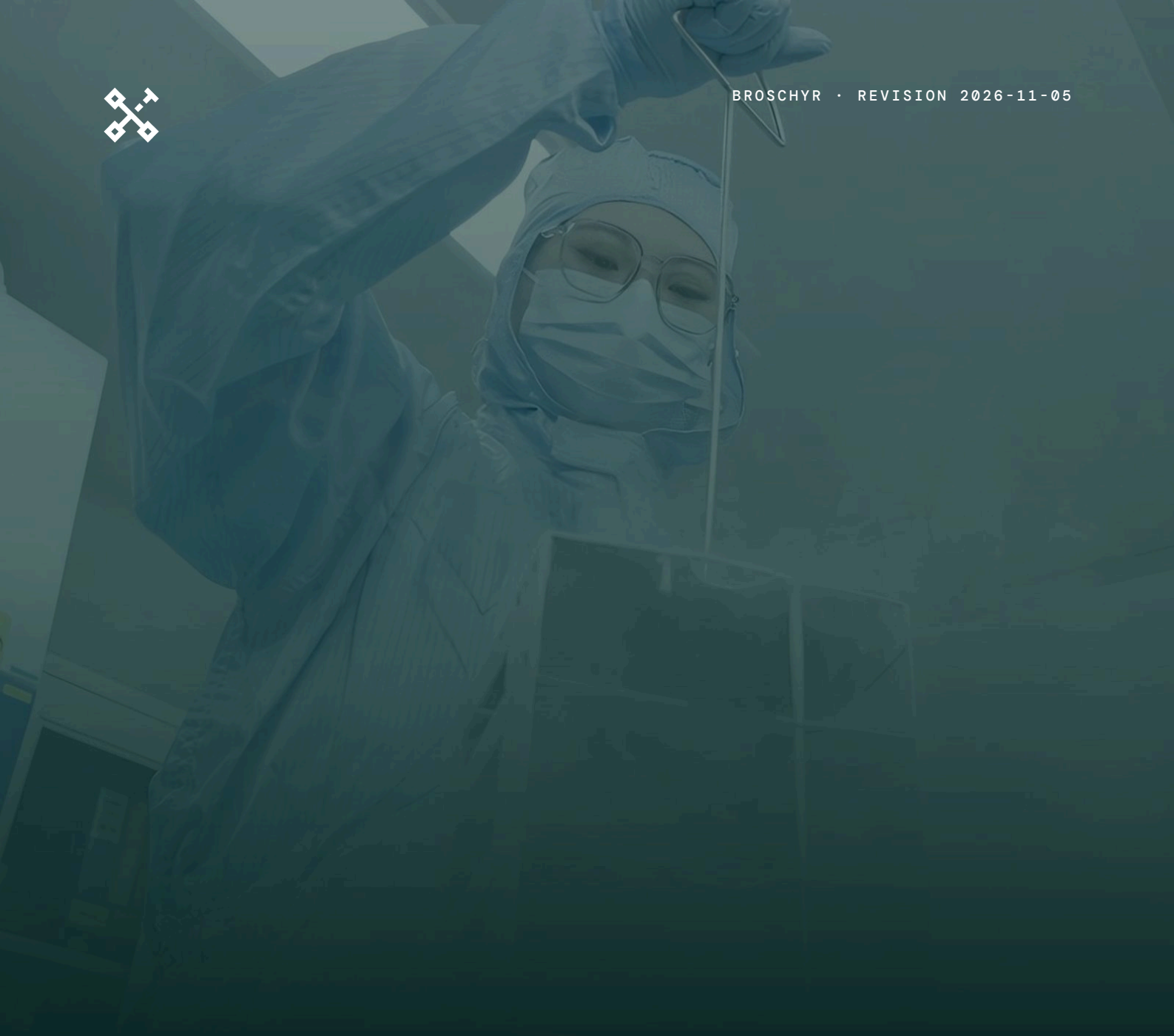


FÖR ER SOM FÖRVARAR PROVER I ULTRAKYLA

Skydda det som inte går att ersätta.

En handbok i grundläggande cybersäkerhet för -80-frysar, kvävetankar, kylrum och övervakningen av dem.

Innehåll

Klicka på en rubrik för att gå direkt till sidan.

01 **Till er som förvarar prover** — Sidan 3
Vem broschyren är skriven för och tre saker att göra i dag

02 **Riskerna** — Sidan 4
Systemen i kylkedjan och hur angripare brukar lyckas

03 **Checklista** — Sidan 5
Åtta vanor för säker förvaring

04 **Var står ni i dag?** — Sidan 6
Inventera utrustningen och se var ni står

05 **Ansvar och regler** — Sidan 7
Vem som ansvarar för vad och vilka regler som gäller

06 **Fjärrsupport** — Sidan 9
Frågor att ställa till era leverantörer

07 **Frysar, tankar och larm** — Sidan 10
Skydda frysarna, larmkedjan och nätverket

08 **Om något händer** — Sidan 11
Vad ni gör om en frys larmar och vilka ni ringer

09 **Ord och hjälp** — Sidan 12
Ord att kunna, mer information och hur Xertified kan hjälpa

Har ni bara fem minuter? Börja med Gör det här i dag på sidan 3.

Byggd på NCSC:s råd

Broschyren följer Nationellt cybersäkerhetscenters (NCSC) fördjupade råd för att skydda OT-miljöer. Den tar också hänsyn till de regelverk som vi beskriver på xertified.se/regelefterlevnad. Tack till NCSC för vägledningen. NCSC har inte granskat broschyren.

Proverna går inte att ta om

Ägg och embryon, en patients egna celler, prover i en biobank och unika frön går inte att ersätta. De förvaras i frysar på -80 °C, så kallade ULT-frysar, och i kvävetankar ned till -196 °C.

Frysarna, kvävetankarna och kylrummen är uppkopplade. De skickar larm och data, ofta till tillverkarens molntjänst. Leverantörer når dem på distans för service. En angripare kan också använda varje sådan väg in.

Den här broschyren hjälper er att skydda förvaringen. Det mesta handlar om att ställa rätt frågor till rätt person. Små steg gör stor skillnad.

Broschyren är skriven för

- sjukhusens laboratorier och IVF-kliniker
- biobanker, stamcells- och vävnadsbanker
- läkemedel och bioteknik, också cell- och genterapi
- företag som driver kliniska prövningar och centrallaboratorier
- blodcentraler och plasmaföretag
- universitet och forskningsinfrastruktur
- myndigheter med laboratorier
- grossister och kylkedjelogistik
- djursjukhus, veterinärlabb och avel
- genbanker för frön och växter

GÖR DET HÄR I DAG · TRE SAKER

1. **Testa larmet.** Gör ett provlarm och se att det når en person, också på natten och på helgen.
2. **Fråga vem som når frysarna på distans.** Fråga tillverkaren, leverantören av övervakningen och kylentreprenören.
3. **Ta reda på var övervakningen finns.** Servern som skickar larmen ska inte stå i samma nätverk som kontorets datorer.

Hela kylkedjan är uppkopplad

Förvaringen bygger på många system som är anslutna till ett eller flera nätverk. Om larmet inte är aktiverat märker ingen att temperaturen stiger.

-80-frysar

De skickar data, ofta till tillverkarens molntjänst.

Kvävetankar

Styrningen fyller på kväve och larmar. Ändrade larmgränser märks sent.

Kylrum och kylmaskiner

En kylentreprenör sköter dem ofta på distans.

Övervakningen

Den skickar larmen. Om den slås ut tystnar larmen.

Automatiska provlager

Leverantören når lagrets dator på distans.

Syrgasvakter och passersystem

De skyddar personalen och styr vem som kommer in.

Så brukar angripare lyckas

- **Via en leverantör.** Angriparen tar sig in hos leverantören och kommer vidare därifrån.
- **Utrustningen syns på internet.** Angripare söker hela tiden efter den.
- **Fabrikens lösenord sitter kvar.** Sådana lösenord går ofta att hitta på internet.
- **Allt sitter i samma nätverk.** Ett angrepp mot kontorets datorer når övervakningen.
- **Larmet är avstängt** eller går via samma nätverk som angrips.
- **Ingen ser något.** Ingen vet vem som ändrade en inställning.

DET HÄR HAR HÄNT

- Angripare tog sig in via en kylleverantör och ändrade temperaturen i kylrum för blodplasma. Larmen upptäckte det i tid.
- Fjärrlarmet på en kvävetank var avstängt när tanken slutade kyla. Tusentals ägg och embryon gick förlorade.
- Ett utpressningsprogram slog ut ett labbs it-system i månader. Tusentals besök och operationer sköts upp.

Åtta vanor för säker förvaring

Börja här. Varje vana gör det svårare för en angripare och lättare för er att upptäcka ett fel i tid.

01

Vet vad som är uppkopplat

Gör en lista över frysar, tankar, kylrum, loggrar och servrar som är anslutna till nätverket.

02

Inget ska nås från internet

Be leverantörerna kontrollera att ingen utrustning går att nå direkt från internet.

03

Ha ett oberoende larm

Larmet ska fungera även om frysens styrning, nätverket eller strömmen faller bort.

04

Testa larmkedjan

Gör ett provlarm regelbundet. Kontrollera att någon svarar och att inget larm är avstängt.

05

Byt lösenord och logga in säkert

Varje enhet ska ha ett eget, starkt lösenord. Fjärråtkomst ska kräva en app eller en hårdvarunyckel, inte sms.

06

Fjärråtkomst bara vid behov

Leverantören ska bara komma in när det finns ett ärende, och bara till sin egen utrustning.

07

Dela upp och bevaka nätverket

Frysar, övervakning och kylrum ska ha egna delar av nätverket. Okänd trafik ska ge larm.

08

Ha en plan och öva den

Bestäm vart proverna flyttas och vem som gör det. Öva det, också utan nätverk.

Tips: Gå igenom checklistan tillsammans med labbet, it, medicinteknik och fastigheten. Ofta äger ingen av dem hela kedjan.

Inventera förvaringen

Skriv upp den utrustning som är uppkopplad. Fråga leverantören om ni inte vet svaret.

Utrustning	Leverantör och telefon	Går att nå från internet?	Vem når den på distans?
-80-frysar			
Kvävetankar och påfyllning			
Kylrum och kylmaskiner			
Övervakning och loggrar			
Larm till jour eller larmcentral			
Automatiskt provlager			
Syrgasvakter och ventilation			
Annat:			

Hur säker är er förvaring?

Påstående	Bra	Okej	Inte än
Vi vet vilken utrustning som är uppkopplad.	☐	☐	☐
Ingen utrustning går att nå direkt från internet.	☐	☐	☐
Larmet fungerar även om nätverket faller bort.	☐	☐	☐
Vi vet vilka leverantörer som har fjärråtkomst.	☐	☐	☐
Vi vet vart proverna flyttas om en frys slutar fungera.	☐	☐	☐

Börja med det ni har kryssat i under Inte än.

Vem ansvarar för vad?

Labbet äger proverna. Men it, medicinteknik, fastigheten eller en leverantör kan sköta frysarna, nätverket och kylrummen. Ta reda på vem som ansvarar för varje del.

System	Labbet	It	Medicinteknik	Fastigheten	Leverantör
-80-frysar	☐	☐	☐	☐	☐
Kvävetankar och kväve	☐	☐	☐	☐	☐
Kylrum	☐	☐	☐	☐	☐
Övervakning och larm	☐	☐	☐	☐	☐
Nätverket	☐	☐	☐	☐	☐
Fjärråtkomst	☐	☐	☐	☐	☐

> **Skriv in det i avtalet.** Kom överens om vem som byter lösenord, installerar uppdateringar och stänger fjärråtkomsten när ett uppdrag är slut.

Beslut som påverkar säkerheten

- Utgå från att utrustningen har sårbarheter. Den får sällan säkerhetsuppdateringar i tid.
- Gå igenom inställningarna. Lita inte på att fabrikens inställningar är säkra.
- Spara loggarna så länge att ni kan utreda en incident i efterhand.
- Skriv ned varje beslut som sänker säkerheten och varför. Se över besluten regelbundet.

Regler att läsa mer om

Tabellen visar vilka regelverk som brukar beröra life science och laboratorier.

En fylld ring (●) betyder att ni bör läsa först. En tom ring (○) betyder att regeln också kan beröra er, till exempel via kunder, leverantörer eller inköp.

Regelverk	Läs	Vad det är
NIS2	● först	EU:s direktiv om cybersäkerhet. I Sverige gäller det genom cybersäkerhetslagen.
CER	● först	EU:s direktiv om motståndskraft i samhällsviktiga tjänster.
GMP och bilaga 11	● först	EU:s regler för datoriserade system i läkemedelsproduktion.
IEC 62443	○ också	Internationell standard för säkerhet i industriella system.
ISO 27001	○ också	Standard för hur en organisation styr sin informationssäkerhet.
NIST	○ också	Vägledningar från USA för säkerhet, bland annat i OT.
21 CFR Part 11	○ också	FDA:s regler för elektroniska journaler och underskrifter.

Särskilt för förvaring av prover

- **Biobankslagen.** Prover ska förvaras så att de inte riskerar att förstöras. Obehöriga ska inte få tillgång till dem.
- **SoHO-förordningen.** EU:s nya regler för material från människor gäller från 7 augusti 2027. De gäller till exempel blod, plasma, vävnader och celler.
- **GMP och 21 CFR Part 11.** Inom läkemedel ska temperaturdata vara tillförlitliga och gå att spåra.
- **NIS2 och cybersäkerhetslagen.** Sjukvård och läkemedelstillverkning kan omfattas. Lagen ställer också krav på säkerheten hos leverantörer.

Vilka regler som gäller just er beror på till exempel storlek, uppdrag och kunder. Det här är vår tolkning, inte juridisk rådgivning. Se tabellen för alla branscher.

Leverantörer som når utrustningen på distans

Tillverkaren av frysen, leverantören av övervakningen och kylentreprenören behöver ofta nå sin utrustning. Det ger snabbare service. Men en angripare kan också använda varje väg in, ibland via leverantören.

Frågor att ställa till era leverantörer

1. Hur når ni vår utrustning? Via en molntjänst, en öppen port, ett delat konto eller en säker anslutning?
2. Vilka data skickas till er molntjänst, och vem hos er kan se dem?
3. Kan ni ändra inställningar eller larmgränser på distans?
4. Har varje tekniker en egen inloggning, med app eller hårdvarunyckel?
    - Delar ni ut inloggningar till era underleverantörer? Har i så fall varje person hos dem en egen inloggning?
5. Kan vi godkänna varje anslutning innan den öppnas?
6. Kan ni visa vem som anslöt, när och vad som ändrades?
7. Hur länge får utrustningen säkerhetsuppdateringar?

Bra svar

- Vi ansluter bara när ni har ett ärende.
- Varje tekniker har en egen inloggning, även hos våra underleverantörer.
- Vi når bara vår egen utrustning.

Varningstecken

- Frysen har en öppen port. Det har alltid fungerat.
- Alla tekniker använder samma lösenord.
- Vi kan ändra allt på distans.
- Vi vet inte.

Läs om säker fjärråtkomst utan öppna portar

Skydda frysarna och larmkedjan

-80-frysar och kylrum

Styrningen håller temperaturen och skickar larm. Om någon ändrar temperaturen ska det synas direkt.

Kvävetankar

Statusen för påfyllningen ger den tidigaste varningen. Kontrollera larmgränserna efter varje service.

Övervakningen

Ha ett larm som fungerar även om frysen, nätverket eller servern slutar fungera.

Dela upp nätverket

Om allt sitter i samma nätverk kan ett angrepp mot kontorets datorer nå övervakningen. Dela därför upp utrustningen i skilda delar. Varje del når bara det den behöver. Läs om att dela upp nätverket



Så här gör ni

- Fråga leverantörerna om någon utrustning går att nå direkt från internet. Svaret ska vara nej.
- Låt frysen bara nå tillverkarens molntjänst och inget annat.
- Skicka larmet på två vägar, till exempel via nätverket och via mobilnätet.
- Installera skydd mot skadlig kod på servern för övervakningen. Låt det först bara larma.
- Se till att larmen når någon dygnet runt, också på helger.

VALIDERAD UTRUSTNING?

Utrustning i en validerad process ändras ogärna. Ett skydd framför den behöver inte ändra något i den.

TÄNK EFTER

Om någon tar över servern för övervakningen, vem märker då att en frys blir varm?

Om en frys larmar eller något verkar fel

1. **Rädda proverna först.** Följ er plan och flytta proverna till en frys eller tank som fungerar.
2. **Kontrollera temperaturen på plats** med en termometer som inte är ansluten till nätverket.
3. **Ta reda på vad som påverkas.** En frys, ett kylrum, larmet eller hela övervakningen?
4. **Ring leverantörens jour.** Berätta vad ni ser och när det började.
5. **Stäng fjärråtkomsten** tillsammans med leverantören tills ni vet vad som har hänt.
6. **Dokumentera.** Skriv ned vad som hände, när, vilka prover som berördes och vad ni gjorde. Följ er rutin för avvikelser.
7. **Polisanmäl** angreppet på polisen.se eller på telefon 114 14.
8. **Rapportera incidenten** till CERT-SE på cert.se. Följ också de krav på rapportering som gäller er verksamhet.

Förbered er redan nu

Fyll i listan och sätt upp den där personalen ser den.

Kontakt	Namn	Telefon
Frysleverantörens jour		
Leverantör av övervakningen		
Kylentreprenör		
Kväveleverantör		
It-jour		
Fastighetens jour		
Ansvarig för proverna		

Ord att kunna

-80-frys	En frys som håller omkring -80 °C. Den kallas också ULT-frys, efter engelskans ultra-low temperature.
Larmkedja	Vägen från givaren i frysen till en person som gör något.
Hårdvarunyckel	En liten dosa för inloggning, till exempel en YubiKey. Den sätts i datorn eller hålls mot den.
Öppen port	En öppning i brandväggen som släpper in trafik från internet.
Fabrikens lösenord	Lösenordet som utrustningen har när den levereras. Det går ofta att hitta på internet.
Utpressningsprogram	Skadlig kod som låser datorer och data och kräver en lösensumma. Det kallas också ransomware.
Validering	Kontroll som visar att utrustningen fungerar som den ska. Varje ändring kan kräva en ny kontroll.

Mer information

cert.se	Sveriges nationella funktion för it-incidenter. Här rapporterar ni en incident.
NCSC om OT	Nationellt cybersäkerhetscenter. Fördjupade råd för att skydda styrsystem och annan uppkopplad utrustning.
polisen.se	Polisanmälan. Telefon 114 14, vid akut fara 112.
biobanksverige.se	Stöd och vägledning om biobankslagen.

Så kan Xertified hjälpa

Vi sätter ett lås framför frysar, kvävetankar, loggrar och servern för övervakningen. Utrustningen syns inte för obehöriga och når bara det den behöver. XoT-Clients kan logga in med YubiKey eller smart kort.

Leverantören får åtkomst till rätt utrustning under en bestämd tid. Ni kan godkänna varje anslutning och se vem som var inne. Utrustningen ändras inte. XoT mäter inte temperaturen och ersätter inte ert larm.

xertified.se/branscher/life-science · info@xertified.com · 018-265 06 06

Boka ett möte eller en demo