

BIOMEDICAL AND BIOTECHNOLOGY

Secure IT for Research Labs Checklist

Protect intellectual property, keep instruments online, and stay audit-ready.

Labs depend on instruments, large data sets, and collaboration with partners outside the building. Your research data is your company. This checklist covers the IT and security foundations that let a lab move fast without leaving the door open.

How to use it: tick what you have in place today. Anything left unticked is a conversation worth having.

01 Lab infrastructure

- ☐ **Instrument PCs on an isolated network segment**
Many run older operating systems that cannot be patched.
- ☐ **High-capacity storage for raw and processed data, sized for growth**
Sequencing and imaging data grows faster than budgets.
- ☐ **Reliable Wi-Fi and wired drops planned with the lab layout**
Instruments move. The network should keep up.
- ☐ **Battery backup on instruments, storage, and network gear**
Power blips can ruin long runs.
- ☐ **Secure remote access for researchers and partners**
No open remote desktop ports on the internet.

02 Protect data and IP

- ☐ **Role-based access to research data, with access reviews**
Departing staff and contractors lose access the same day.
- ☐ **Multi-factor authentication on email, cloud, and remote access**
Research IP is a target for theft.
- ☐ **Encrypted file transfer for sharing with CROs and partners**
No personal file-sharing accounts.
- ☐ **Endpoint detection and response monitored 24/7**
Exceptions documented for validated instrument PCs.
- ☐ **Audit trails and electronic signatures where 21 CFR Part 11 applies**
Know which systems are in scope.

03 Scale and recover

- ☐ **Automated onboarding and offboarding for staff and contractors**
Labs grow in bursts.
- ☐ **Backups of research data with an off-site or immutable copy**
Test restores of large data sets, not just documents.
- ☐ **Cloud compute plan for analysis and AI workloads**
Burst to the cloud instead of buying idle servers.
- ☐ **Asset inventory including instruments and their software versions**
Validation depends on knowing what changed.
- ☐ **Quarterly IT roadmap tied to funding milestones**
Plan capacity before the next round lands.

Red flags we see most

- Instrument PCs share a network with guest Wi-Fi.
- Raw data lives on one external drive.
- Collaborators share data through personal accounts.
- Nobody knows which systems are validated.

Where to start

Segment the instrument network first. It protects the machines you cannot patch and is usually a one-day project.

Want a second set of eyes?

Book a free 30-minute technical assessment. A senior engineer walks through this checklist with you and tells you what to fix first. No sales script, no obligation.

Book a technical assessment

(617) 322-5155

bostonmit.com/it-assessment