|  |  |  |
| --- | --- | --- |
| Security Domain | Requirements | Steps for Lab IT Teams |
| System Hardening and Updates | Regularly update and patch all devices connected to CITNet. | * Configure systems to apply updates automatically or designate responsible individuals for manual updates.
* Harden devices following vendor guidelines.
 |
| Backups | Routine backups to prevent data loss. | * Use external drives for manual backups and disconnect immediately after.
* Avoid internet browsing during backups.
* Consult IMSS for automated backups.
 |
| Security Awareness | Avoid installing software without considering risks. | * Take Cyber Security training available through MyLearn.
* Maintain good security habits and recognize common scams.
 |
| Endpoint Protection | All endpoints must have anti-malware protection. | * Install IMSS EDR CrowdStrike on Caltech-owned devices.
* Enable Defender or similar solutions on personal devices.
* Apply security updates immediately.
 |
| Account Management and Authentication | Enable SSO and MFA wherever possible. | * Collaborate with IMSS to implement Duo MFA.
* Use strong, unique passwords.
* Configure inactivity settings.
* Use Caltech-assigned accounts.
* Avoid non-Caltech activities.
 |
| Personal Computing & Instrument Controllers | Use systems for intended purposes only. | * Avoid personal activities on lab resources.
* Place instrument controllers in their own network segment with restricted access.
 |
| Least Privilege | Give users only the access they need. | * Do not assign unnecessary roles or capabilities.
 |
| Remote Access | Disable remote access if not needed. | * Use reliable tools like Windows RDP.
* Configure strong passwords and MFA.
* Block off-campus traffic and use VPN.
* Secure connections with SSH tunneling when using VNC.
 |
| Secrets Management  | Store secrets safely using a password manager and encrypt data | * Use unique passwords for each account.
* Encrypt data at rest and in transit.
 |
| Central Logging | Send security log events to IMSS Information Security. | * Configure systems to send syslog data to IMSS log servers.
 |
| Internet of Things | Restrict access to IoT devices. | * Change default administrator passwords.
* Keep devices up to date.
* Block off-campus traffic.
 |

**Need Assistance?** Contact IMSS Information Security at security@caltech.edu

 [Learn more Lab Security Recommendations](https://www.imss.caltech.edu/services/security/recommendations/lab-security)