| Security Domain | Requirements | Steps for IT resources |
|---|---|---|
| **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.<br>• Harden devices following vendor guidelines. |
| **Backups** | Routine backups to prevent data loss. | • Use external drives for manual backups and disconnect immediately after.<br>• Avoid internet browsing during backups.<br>• Consult IMSS for automated backups. |
| **Security Awareness** | Avoid installing software without considering risks. | • Take Cyber Security training available through MyLearn.<br>• 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.<br>• Enable Defender or similar solutions on personal devices.<br>• Apply security updates immediately. |
| **Account Management and Authentication** | Enable SSO and MFA wherever possible. | • Collaborate with IMSS to implement Duo MFA.<br>• Use strong, unique passwords.<br>• Configure inactivity settings.<br>• Use Caltech-assigned accounts.<br>• Avoid non-Caltech activities. |
| **Personal Computing & Instrument Controllers** | Use systems for intended purposes only. | • Avoid personal activities on lab resources.<br>• 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.<br>• Configure strong passwords and MFA.<br>• Block off-campus traffic and use VPN.<br>• 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.<br>• 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.<br>• Keep devices up to date.<br>• Block off-campus traffic. |

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

Learn more about Researcher Security Recommendations