



Lasar Minimum Technology Standards

Version: June 2026

<i>Lasar Minimum Technology Standards</i>	1
1. Introduction	2
2. Compliance Levels	2
3. General Principles.....	3
4. Network Infrastructure	3
5. Internet Connectivity	4
6. Workstations.....	4
7. Servers	5
8. Supported Software.....	5
9. Microsoft 365	7
10. Identity & Access	8
11. Endpoint Security	8
12. Email Security.....	9
13. Backup & Disaster Recovery	9
14. Patch Management.....	9
15. Domain & DNS.....	9
16. Equipment Lifecycle	10
17. Lasar Preferred Technology & Security Stack	10
18. Minimum Security Baseline.....	11
19. Exceptions	11
20. Our Commitment.....	12



1. Introduction

At Lasar, we believe technology should be an enabler—not a source of risk, downtime or frustration.

These Minimum Technology Standards define the baseline hardware, software and security controls that we recommend for all managed clients. They have been developed through years of supporting Australian businesses and reflect industry best practice.

By standardising on proven technologies and maintaining modern, supported systems, we can provide faster support, improved cybersecurity, lower operational risk and a better overall customer experience.

Environments that do not meet these standards may still be supported; however, additional charges, reduced service levels or remediation recommendations may apply.

2. Compliance Levels

Gold – Lasar Preferred

The environment fully aligns with the Lasar Preferred Technology & Security Stack.

Gold environments benefit from:

- Full proactive management
- Best-practice cybersecurity
- Fastest support response
- Predictable lifecycle management
- Standard SLA eligibility
- Simplified troubleshooting
- This is the target standard we recommend for all managed clients.

Silver – Supported

The environment uses enterprise-grade technologies that differ from Lasar's preferred stack but still meet our minimum standards.

Silver environments receive:

- Full managed support
- Standard SLA commitments
- Enterprise-grade protection
- Support for approved alternative platforms



● Bronze – Legacy

The environment contains unsupported, consumer-grade or end-of-life technologies.

Support may be provided on a best-effort basis and may incur additional charges.

Bronze environments may not qualify for standard SLA commitments until remediation has been completed.

3. General Principles

Technology should:

- Be vendor supported
- Receive security updates
- Be appropriately licensed
- Be business-grade
- Be capable of remote management
- Meet modern cybersecurity standards
- Consumer-grade equipment should not be relied upon for business-critical functions.

4. Network Infrastructure

Firewalls

Preferred:

- Ubiquiti UniFi Gateway
- Cisco Meraki MX

Firewalls should support:

- VPN
- Automatic firmware updates
- VLANs
- Remote management
- Security logging
- ISP-supplied routers should only be used temporarily.

Switching



Preferred:

- Ubiquiti UniFi
- Cisco Meraki
- TP-Link Omada Business

Managed switches are recommended for all business deployments.

Wireless

Preferred:

- Ubiquiti UniFi
- Cisco Meraki

Wireless should support:

- WPA3 where available
- Guest isolation
- Central management
- Business-grade hardware
- Consumer mesh systems are discouraged.

5. Internet Connectivity

Recommended:

- Business-grade NBN or fibre
- Static IP where required
- 4G/5G failover where business continuity requires it

6. Workstations

Windows Minimum specifications:

- Windows 11 Pro
- 16GB RAM
- SSD
- TPM 2.0



- Secure Boot
- Microsoft-supported hardware
- Windows Home editions are not recommended.

Apple macOS

- Supported macOS version
- Apple Silicon preferred
- 8GB RAM minimum

7. Servers

Servers should:

- Run supported operating systems
- Be covered by warranty
- Have redundant storage
- Be protected by enterprise backup
- Be monitored by Lasar
- Virtualisation is recommended.

8. Supported Software

Lasar supports current, vendor-supported business software platforms.

Productivity

- Microsoft 365 Apps for Business / Enterprise
- Microsoft Office 2021
- Microsoft Office 2024
- Outlook (Classic)
- New Outlook for Windows
- Microsoft Teams
- OneDrive for Business
- SharePoint Online

Older perpetual versions of Microsoft Office may be supported while still within Microsoft's support lifecycle.



PDF & Document Management

Adobe Acrobat Standard

Adobe Acrobat Pro

Adobe Acrobat Reader

Foxit PDF Editor (current versions)

Web Browsers

Supported:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Safari (macOS)

Browsers should remain on current release channels with automatic updates enabled.

Email Platforms

Preferred:

- Microsoft Exchange Online
- Microsoft 365

Also supported where appropriate:

- Google Workspace
- IMAP (limited support only)
- Mailassure (Lasar)

POP3-based email systems are discouraged and may not be fully supported.

Collaboration

- Microsoft Teams
- Zoom

Accounting & Business Applications

Commonly supported applications include:



- MYOB
- Xero
- QuickBooks
- Reckon
- FileMaker Pro
- Microsoft SQL Server

Industry-specific applications may be supported where vendors provide current support.

Remote Access

Supported:

- Microsoft Remote Desktop
- ScreenConnect (where approved)
- TeamViewer (where approved)
- VPN solutions
- Microsoft RDP with MFA

Internet-exposed RDP is not supported.

Unsupported Software

Lasar may decline support for:

- End-of-life applications
- Unsupported operating systems
- Pirated or unlicensed software
- Legacy Office versions outside Microsoft's support lifecycle
- Obsolete browsers
- Software requiring deprecated security protocols

Where practical, clients will be advised to upgrade before support is provided.

9. Microsoft 365

Recommended licensing:



- Microsoft 365 Business Premium
- Microsoft 365 E3

Security features should include:

- Multi-Factor Authentication
- Microsoft Defender
- Exchange Online Protection
- Conditional Access
- Modern Authentication
- Legacy authentication should be disabled.

10. Identity & Access

Every user should have:

- Individual credentials
- MFA enabled
- Strong passwords or passkeys
- Administrative accounts should be separate from normal user accounts.

11. Endpoint Security

All devices should include:

- Managed Endpoint Detection & Response
- Automatic updates
- Tamper protection

Lasar recommends Huntress Managed EDR with Microsoft Defender.



12. Email Security

Business email should include:

- Advanced spam filtering
- Anti-phishing protection
- SPF
- DKIM
- DMARC

Lasar recommends Barracuda Email Gateway Defense.

13. Backup & Disaster Recovery

Critical data should be protected by:

- Daily backups
- Offsite cloud storage
- 90-day minimum retention
- Quarterly restore testing
- Microsoft 365 should also be independently backed up.

Lasar recommends Cove Data Protection.

14. Patch Management

Operating systems and applications should:

- Automatically update
- Be monitored for failures
- Remain within vendor support

Critical security patches should be applied promptly.

15. Domain & DNS

Business domains should:



- Be client-owned
- Have MFA enabled
- Use Lasar as the DNS provider.

16. Equipment Lifecycle

Equipment

Desktop PCs

Laptops

Servers

Firewalls

Switches

Wireless Access Points

UPS Batteries

Recommended Replacement

5 years

4–5 years

5 years

5–7 years

7 years

5–7 years

3–5 years

17. Lasar Preferred Technology & Security Stack

Category

Firewall

Wireless

Switching

Microsoft Licensing

Microsoft 365 Security

Endpoint Protection

Email Security

Microsoft 365 Backup

Server Backup

Remote Monitoring

Password Management

Documentation

Identity Platform

Preferred Standard

Ubiquiti UniFi Gateway or Cisco Meraki MX

Ubiquiti UniFi

Ubiquiti UniFi

Microsoft 365 Business Premium

Huntress ITDR

Huntress Managed EDR + Microsoft Defender

Barracuda Email Gateway Defense

Cove Data Protection

Cove Data Protection

Datto RMM

Passportal

Hudu

Microsoft Entra ID



Authentication

Multi-Factor Authentication for all users

Email Authentication

SPF + DKIM + DMARC

Remote Access

Zero Trust VPN

18. Minimum Security Baseline

Every managed client should implement:

- Multi-Factor Authentication for all users
- Managed EDR
- Enterprise email filtering
- Independent Microsoft 365 backup
- Offsite backup of servers and critical data
- Automatic patch management
- Security awareness training
- Strong password or passkey policies
- SPF, DKIM and DMARC
- Secure remote access
- No Internet-exposed RDP services
- Security should be implemented in layers rather than relying on any single product.

19. Exceptions

Lasar recognises that some organisations have unique requirements. Exceptions may be approved following a documented risk assessment but may:

- Increase support costs
- Affect SLA commitments
- Require acceptance of additional business risk
- Be periodically reviewed



20. Our Commitment

Our objective is not merely to support IT systems but to help clients build secure, reliable and resilient technology environments.

Organisations that align with these standards typically experience:

- Less downtime
- Better cybersecurity
- Faster support
- Easier upgrades
- Lower long-term costs
- Greater confidence in their technology investment

These standards will continue to evolve as technology and cybersecurity best practices change.