mint TECHNOLOGY Audit

Systems Audit Report (KSC)

Report **AUD-02944** Customer **Kaleidoscope Consulting** Audited **16 October 2026**



Based on 27 items assessed across 4 areas



Connectivity & Devices
Good
6 items · 2 to address



Security & Protection
Needs work
9 items · 4 to address



Data & Recovery
Critical
3 items · 3 to address



People, Process & Planning
Needs work
9 items · 6 to address

We've completed your systems audit

Overall, Kaleidoscope Consulting's IT environment rates Needs work. We assessed 27 items across 4 areas: 12 are working well, 12 need work and 3 are critical. The most important things to deal with first are business data backups, individual logins and emergency response plan.



Got questions? Contact your account manager
Cameron Hicks · 09-222-0220

How to read the ratings

- **Excellent**
  Working well. No action needed.
- **Good**
  Solid, with minor tidy-ups possible.
- **Needs work**
  Functional, but gaps that should be planned for.
- **Critical**
  A real risk to your business. Fix first.

What to do first

The highest-impact actions from this audit, in the order we'd tackle them.

1. **Business data backups**
   Add an offsite/cloud backup copy and schedule quarterly restore tests.

   Do now · Medium effort

2. **Individual logins**
   Give every user their own login and retire the shared accounts.

   Do now · Low effort

3. **Emergency response plan**
   Create a one-page plan with key contacts and first steps.

   Within 3 months · Low effort

4. **Sign-in verification (MFA)**
   Enforce MFA for all Microsoft 365 users.

   Do now · Low effort

5. **Wi-Fi coverage**
   Add an access point covering meeting rooms and reception, or reposition the existing one.

   Within 3 months · Medium effort

Detailed findings

Every area we checked. Select an item for evidence, impact and our recommendation.

Connectivity & Devices

How your office connects, and the kit it runs on · **Good**

Wi-Fi coverage

Coverage drops in meeting rooms and reception

Needs work

2
weak-signal areas

1
access point

What we found

Signal is good in the main work areas but weak in the meeting rooms and reception.

Why it matters

Dropped video calls and slow connections where clients and visitors spend time.

What we recommend

Add an access point covering meeting rooms and reception, or reposition the existing one.

Computer age & warranty

Some devices are nearing end-of-life

Needs work

5 of 14
devices over 5 years old

3
out of warranty

What we found

A portion of your devices are over five years old and no longer under warranty. They still work but are slower and less reliable.

Why it matters

Ageing devices fail at inconvenient times and slow staff down.

What we recommend

Budget for staged replacement, starting with the oldest devices, over 12 to 24 months.

Office network equipment

Stable, but not fully labelled or documented

Good

2
managed switches

What we found

Switches are managed and stable. Patch panel labelling and a network diagram are missing, which slows down fault-finding.

Why it matters

Undocumented networks take longer to fix when something breaks.

What we recommend

Label patch panels and produce a simple network diagram.

Battery backup power

Key equipment covered; battery age unknown

Good

1
UPS, covers comms cabinet and NAS

What we found

The comms cabinet and NAS are on a UPS. We couldn't confirm battery age or the last test date.

Why it matters

A worn-out battery gives no protection during a power cut or surge.

What we recommend

Confirm battery age and schedule a runtime test.

Internet connection

Reliable, with no bottlenecks found

Excellent

100%
uptime, last 30 days

0
congestion events

What we found

Your primary fibre connection stayed up for the whole 30-day test window. Speed tests across several devices showed no bottlenecks.

Why it matters

Staff can rely on cloud apps, phones and video calls without interruption.

What we recommend

No change needed. Consider a low-cost 4G/5G failover so a fibre cut doesn't stop the office.

Phone call quality

Calls are clear and voice traffic is prioritised

Excellent

QoS
voice traffic prioritised

What we found

Test calls were clear and reliable. Quality of service is set up so voice traffic is prioritised on your network.

Why it matters

Customers judge you by how calls sound. Poor quality costs credibility.

What we recommend

No action needed. Re-test after any network or internet change.



Security & Protection

Keeping threats out and limiting the damage · **Needs work**

Sign-in verification (MFA)

Enabled for some users, not everyone

Needs work

9 of 14
users with MFA

0
admins unprotected

What we found

MFA is enabled for administrators and some staff, but five users don't have it.

Why it matters

A stolen password is enough to reach email and files for those five accounts.

What we recommend

Enforce MFA for all Microsoft 365 users.

Password storage

No company-wide password manager

Needs work

0
users on a password manager

What we found

Staff keep passwords in browsers or spreadsheets. There is no shared, managed password tool.

Why it matters

Reused and shared passwords make breaches easier and offboarding harder.

What we recommend

Roll out a business password manager and retire shared spreadsheets.

Guest network separation

Guests and staff share one Wi-Fi network

Needs work

1
shared Wi-Fi network

What we found

Guests and staff connect to the same Wi-Fi network.

Why it matters

A visitor's infected laptop could reach your internal systems.

What we recommend

Create a separate guest network with internet-only access.

Staff scam awareness

Informal guidance, no regular programme

Needs work

0
phishing tests run

What we found

Staff receive ad-hoc guidance, but there is no regular training or phishing simulation.

Why it matters

Staff are your most frequent target. Awareness is the cheapest control you can add.

What we recommend

Introduce short quarterly training and simulated phishing.

Network firewall

Business-grade firewall; advanced filtering not enabled

Good

1
business firewall

What we found

A business-grade firewall is in place and receiving firmware updates. Advanced threat filtering isn't switched on.

Why it matters

The firewall is your network's front door. Extra filtering blocks more attacks.

What we recommend

Enable intrusion prevention and web filtering on the existing firewall.

Scam & spam email filtering

Filtering active; link scanning not enabled

Good

On
phishing and spam filter

What we found

Spam and phishing filtering is active. Link and attachment scanning isn't enabled.

Why it matters

Phishing email is the most common way attackers get in.

What we recommend

Review filter settings and enable link and attachment scanning.

Software updates

Automated, with a few stragglers

Good

12 of 14

devices fully up to date

What we found

Most devices update automatically. Two machines are behind by a month or more.

Why it matters

Known weaknesses stay exploitable until they are patched.

What we recommend

Bring the two stragglers up to date and check compliance monthly.

Administrator access

Limited to IT, with a couple of exceptions

Good

2

staff with local admin rights

What we found

Administrator rights are mostly limited to IT. Two staff members keep local admin rights on their own computers.

Why it matters

Admin rights let malware install itself and spread. Fewer admins means less risk.

What we recommend

Remove local admin rights from the two users and use a separate admin account for IT tasks.

Antivirus & malware protection

Managed protection on every audited device

Excellent

14 of 14
devices protected

0
outdated definitions

What we found

All audited Windows devices have centrally managed antivirus and endpoint protection, and definitions are current.

Why it matters

The first line of defence against malware and ransomware is in place and working.

What we recommend

No action needed.

Data & Recovery

Getting your business back up after something goes wrong · **Critical**

Business data backups

Backups are local-only and haven't been restore-tested

Critical

0
offsite copies

6+ mo
since last restore test

What we found

Backups go to an onsite NAS only. There is no offsite or cloud copy, and the last successful restore test was over six months ago.

Why it matters

A fire, theft or hardware failure could permanently destroy your business data, and you won't know whether a restore works until you need it.

What we recommend

Add an offsite/cloud backup copy and schedule quarterly restore tests.

Emergency response plan

No written plan for a security incident or outage

Critical

None

written plan

What we found

There is no written plan covering who to call, what to do first, or how to communicate during an incident.

Why it matters

Response would be ad hoc and slow, which increases downtime and cost.

What we recommend

Create a one-page plan with key contacts and first steps.

Microsoft 365 data protection

Email and files rely on Microsoft's native retention

Needs work

0

independent M365 backups

What we found

Microsoft 365 mail and files are not backed up independently. Recovery depends on Microsoft's limited retention.

Why it matters

Accidental deletion or a compromised account can mean permanent loss of email and files.

What we recommend

Add an independent Microsoft 365 backup service.



People, Process & Planning

How IT is run, supported and governed day to day · **Needs work**



Individual logins

Multiple staff share logins

Critical

3

shared accounts in use

What we found

Shared accounts are used for key systems, which makes it impossible to know who did what.

Why it matters

You can't audit access or cleanly remove one person's access, and you may fall short of compliance obligations.

What we recommend

Give every user their own login and retire the shared accounts.

Software licences

Functional but inconsistent

Needs work

Mixed

personal and business emails on licences

What we found

A mix of personal and business email addresses are used for licensed software.

Why it matters

Licences tied to personal accounts are hard to manage and are lost when staff leave.

What we recommend

Standardise on business accounts (e.g. Microsoft 365 Business).

System records

Partial and out of date

Needs work

Partial

asset and credential records

What we found

Key system information exists but is incomplete and spread across several places.

Why it matters

When the one person who knows the setup is away, fixes take longer and cost more.

What we recommend

Keep asset, licence and configuration records in one documented place.

Leaver & access reviews

Access is role-based but never reviewed

Needs work

Never

last access review

What we found

Access is broadly role-based but hasn't been reviewed, so leavers and role changes may have lingering access.

Why it matters

Unused access is an easy target and an easy mistake.

What we recommend

Review access twice a year and on every leaver.

Written security policies

Some guidance, nothing formal

Needs work

0
signed-off policies

What we found

Informal guidance exists but there are no documented, communicated security policies.

Why it matters

Staff can't follow rules that aren't written down, and clients increasingly ask for them.

What we recommend

Adopt a short set of core policies (acceptable use, passwords, data handling).

Privacy breach readiness

Reporting obligations not yet mapped

Needs work

Unclear
who notifies, and when

What we found

There is no documented process for notifying the Privacy Commissioner and affected people after a notifiable privacy breach.

Why it matters

Under the Privacy Act 2020, notifiable breaches must be reported as soon as practicable.

What we recommend

Document the notification steps as part of the emergency response plan.

Scheduled maintenance

Regular, but reporting is light

Good

Monthly

maintenance window

What we found

Maintenance happens on a regular schedule. Management reporting is limited.

Why it matters

Visibility helps you plan spend and spot trends.

What we recommend

Add a short monthly health summary for management.

IT roadmap

Regular advice; nothing written down

Good

None

documented 12-month plan

What we found

IT decisions are discussed regularly, but there is no written 12-month plan.

Why it matters

A roadmap avoids surprise spending and keeps IT aligned with business goals.

What we recommend

Produce a simple 12-month IT roadmap and budget.

IT support responsiveness

Quick response, clear expectations

Excellent

< 1 hr

median first response

What we found

Requests are acknowledged quickly and staff know how to get help.

Why it matters

Minor issues don't turn into lost hours.

What we recommend

No action needed.

About this report

This is a structured advisory assessment based on our technicians' observations, tooling output and conversations with your team. It is not a formal compliance audit, certification or penetration test.

How scores work

Each item is rated against a fixed four-level scale so results are consistent between audits. Domain and overall ratings are the average of assessed items; items not assessed are excluded rather than marked down.