Microsoft 365 Security and Backup Checklist

Microsoft 365 is powerful, but it still needs proper security, cleanup, access control and backup planning.

Use this checklist to review common gaps in email, SharePoint, OneDrive, Teams, users, groups and recovery.

REVIEW ACCOUNT ACCESS	PROTECT EMAIL AND FILES	CONFIRM BACKUP REALITY
Check MFA, admin rights, former employees, shared mailboxes and risky sign-ins.	Review email security, phishing protection, SharePoint, OneDrive and Teams sharing.	Understand what Microsoft does and does not protect by default.

Microsoft 365 Is Not Set It and Forget It

Many businesses assume Microsoft 365 automatically handles security, backup and governance. Microsoft provides the platform, but businesses still need to configure access, monitor risk, manage users and protect important data.

User and Access Control Checklist

Access Review Items

- MFA enabled for all users.
- Admin accounts separated from daily-use accounts.
- Former employees removed.
- Shared mailboxes reviewed.
- Guest users reviewed.
- Conditional access reviewed where applicable.
- Sign-in logs monitored.
- Risky users investigated.
- Password policies reviewed.
- Legacy authentication disabled where appropriate.

Email Security Checklist

Email Security Items

- SPF configured.
- DKIM configured.
- DMARC configured.
- Anti-phishing protection reviewed.
- Suspicious login alerts monitored.
- External sender warnings considered.
- Mail forwarding rules reviewed.
- Shared mailbox permissions reviewed.
- Business email compromise risk reviewed.

SharePoint, OneDrive and Teams Checklist

Collaboration Cleanup

- External sharing settings reviewed.
- Anonymous sharing links restricted where appropriate.
- Sensitive libraries identified.
- Teams ownership documented.
- Old groups reviewed.
- File permissions cleaned up.
- Personal OneDrive business data reviewed.
- Retention settings reviewed.
- Access for former employees removed.

Backup and Recovery Checklist

Recovery Readiness

- Microsoft 365 backup solution reviewed.
- Email backup confirmed.
- SharePoint backup confirmed.
- OneDrive backup confirmed.
- Teams data backup reviewed.
- Restore testing performed.
- Retention expectations documented.
- Ransomware recovery process reviewed.
- Deleted-user data handling documented.

Common Microsoft 365 Risk Areas

Risk Areas

- Too many global admins.
- Former employees still active.
- No third-party backup.
- External sharing too open.
- No DMARC policy.
- Unmonitored forwarding rules.
- Shared accounts.
- Unknown guest users.
- No restore testing.
- Groups and Teams sprawl.

Leadership Questions to Ask

Ownership Questions

- Who owns Microsoft 365 administration?
- Who reviews users and licenses?
- Who monitors risky sign-ins?
- Who confirms backups are working?
- Who handles employee offboarding?
- Who approves external sharing?
- Who reports Microsoft 365 risk to leadership?

NEXT STEP

Need help turning this checklist into action? Schedule a Technology Gap Review with Nevada IT Support.

Schedule a Technology Review at itsupportnv.com/technology-gap-review/