Law Firm IT and Cybersecurity Checklist

Law firms depend on secure email, reliable document access, confidentiality and uptime.

Use this checklist to review the technology areas that protect client data, reduce disruption and support daily legal work.

PROTECT CLIENT CONFIDENTIALITY	REDUCE DOWNTIME RISK	IMPROVE LEGAL WORKFLOW SUPPORT
Review email, document access, permissions and account security.	Evaluate support, backups, internet, phones and business continuity planning.	Review Microsoft 365, case management systems, vendors and onboarding/offboarding.

Why Law Firm IT Needs a Different Standard

Law firms handle sensitive client data, deadlines, court filings, communications, discovery, settlement documents and confidential records.

What Legal IT Support Must Emphasize

IT support for a law firm must focus on uptime, confidentiality, controlled access, backup readiness and user productivity.

Confidentiality and Access Control Checklist

Access Control Items

- MFA enabled for all users.
- Former employees removed immediately.
- Shared accounts eliminated.
- Admin access restricted.
- Client data access reviewed.
- Guest access reviewed.
- File permissions documented.
- Password manager considered.
- User onboarding/offboarding documented.
- Mobile device access reviewed.

Email Security Checklist

Email Protection Items

- Advanced email security enabled.
- SPF configured.
- DKIM configured.
- DMARC configured.
- Suspicious forwarding rules reviewed.
- External sender warnings considered.
- Phishing training provided.
- Business email compromise process documented.
- Email archiving reviewed if needed.

Document and Case Workflow Checklist

Workflow Review Items

- Microsoft 365 permissions reviewed.
- SharePoint/OneDrive structure reviewed.
- Case management integrations documented.
- Dropbox or other file tools reviewed.
- Local files identified.
- Document backup confirmed.
- Scanner/printer workflow reviewed.
- Remote access secured.
- Vendor access documented.

Backup and Business Continuity Checklist

Continuity Items

- Email backup confirmed.
- Cloud file backup confirmed.
- Local computer backup expectations documented.
- Critical systems identified.
- Restore testing performed.
- Internet backup considered.
- Phone system continuity reviewed.
- Recovery time expectations documented.
- Cyber incident response process reviewed.

Legal IT Red Flags

Warning Signs

- Attorney or office manager handles IT alone.
- No tested Microsoft 365 backup.
- Former employees still have access.
- Email security is basic or unknown.
- No formal onboarding/offboarding process.
- Sensitive files live only on local computers.
- Case management vendor access is undocumented.
- No response-time expectations.
- No technology roadmap.

Questions Law Firm Leadership Should Ask

Leadership Questions

- Who owns IT security?
- Who reviews access to client data?
- Who confirms backups are restorable?
- Who handles urgent support?
- Who manages Microsoft 365?
- Who coordinates legal software vendors?
- Who documents users, devices and licenses?
- Who reports technology risk to firm 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/