vijilan
IT Security: Enabled

DMS SECURITY CHECKLIST

10 Questions Every Law Firm Must Answer

About NetDocuments Security

Your document management system holds your firm's most sensitive information—client files, privileged communications, M&A strategies, litigation plans. Use this checklist to assess whether your NetDocuments environment is adequately protected.

Who monitors NetDocuments activity?

- ☐ We have 24/7 SOC monitoring of NetDocuments
- ☐ Our IT team reviews logs periodically
- ☐ No one actively monitors NetDocuments activity
- ☐ I don't know

Why It Matters: Without active monitoring, insider threats, credential compromise, and data exfiltration go undetected until it's too late.

How quickly would you detect a compromised account accessing client documents at 2 AM?

- ☐ Within minutes (real-time alerting)
- ☐ Within hours (next business day review)
- ☐ Days or weeks (during periodic audit)
- ☐ We probably wouldn't detect it

Why It Matters: Attackers who compromise attorney credentials often access systems during off-hours. Without 24/7 monitoring, these intrusions are invisible.

Can you identify if a departing employee downloaded client files before leaving?

- ☐ Yes, we have automated alerts for mass downloads
- ☐ We could investigate if we suspected something
- ☐ No, we have no visibility into download activity
- ☐ I don't know

Why It Matters: Insider data theft by departing employees is the #1 risk to law firms. Most firms discover it months later—if ever.

Do you monitor permission changes in NetDocuments?

- ☐ Yes, all permission changes trigger alerts
- ☐ We review permissions periodically
- ☐ No, we don't monitor permission changes
- ☐ I don't know

Why It Matters: Privilege escalation—users granting themselves access to restricted matters—is a common attack vector and policy violation.

Are NetDocuments logs integrated with your SIEM?

- ☐ Yes, with custom detection rules for legal DMS
- ☐ Yes, but without specific detection rules
- ☐ No, NetDocuments is not integrated
- ☐ We don't have a SIEM

Why It Matters: Without SIEM integration, you cannot correlate DMS activity with endpoint, identity, and network events to detect sophisticated attacks.

Can you prove to clients that their documents are monitored 24/7?

- ☐ Yes, we have audit reports and SOC certification
- ☐ We could explain our security measures verbally
- ☐ No, we don't have documentation
- ☐ Our DMS is not monitored 24/7

Why It Matters: Corporate clients increasingly require proof of security monitoring. Outside counsel guidelines and RFPs ask specifically about DMS security.

What is your response time for critical NetDocuments security alerts?

- ☐ Under 15 minutes (24/7)
- ☐ Within a few hours during business hours
- ☐ Next business day
- ☐ We don't have alerting for NetDocuments

Why It Matters: When credentials are compromised or data exfiltration begins, every minute counts. Delayed response means greater exposure.

Do you have incident response procedures for NetDocuments breaches?

- ☐ Yes, documented procedures with assigned roles
- ☐ We have general incident response procedures
- ☐ No documented procedures for DMS incidents
- ☐ I don't know

Why It Matters: ABA Formal Opinion 483 requires lawyers to investigate breaches promptly. Without procedures, response is delayed and disorganized.

Can you detect if someone accesses a restricted matter they shouldn't?

- ☐ Yes, we have matter-level access monitoring
- ☐ We could investigate after the fact
- ☐ No, we don't monitor matter-level access
- ☐ I don't know

Why It Matters: Unauthorized access to restricted matters—whether by insiders or compromised accounts—creates ethical violations and client exposure.

Does your cyber insurance require DMS monitoring?

- ☐ Yes, and we meet the requirements
- ☐ Yes, but we may have gaps
- ☐ No, it's not required
- ☐ I haven't reviewed our policy requirements

Why It Matters: Many cyber insurance policies now require active monitoring of critical systems. Non-compliance may void coverage when you need it most.

SCORING YOUR RESULTS

8-10 "Yes" STRONG	5-7 "Yes" GAPS EXIST	0-4 "Yes" CRITICAL
Strong DMS security posture. Continue to assess and improve.	Significant gaps exist. Prioritize improvements in areas of weakness.	Critical vulnerabilities. Your firm's client data is at risk. Take immediate action.

HOW DID YOU SCORE?

If you answered "No" or "I don't know" to more than 2 questions, your NetDocuments environment has critical security gaps.

VIJILAN'S NETDOCUMENTS CLOUD CONNECTOR PROVIDES:

24/7 SOC Monitoring • 5-Minute Log Ingestion • 15-MinuteResponse SLA • Pre-built Legal DMS Detection Rules • Compliance Documentation

GET A FREE ASSESSMENT

vijilan IT Security: Enabled