NJSBA PRACTICEHQ Affinity CONSULTING

DATA RECOVERY READINESS – CHECKLIST

❖ IMMEDIATE RESPONSE CHECKLIST

➢ STOP USING THE AFFECTED DEVICE/ACCOUNT

Prevents overwriting recoverable data or spreading damage.

➢ DISCONNECT IF MALWARE IS SUSPECTED

Limits ransomware or destructive sync from reaching more systems.

➢ DO NOT FORMAT, REPAIR, OR REINSTALL

Protects the original evidence and remaining recoverable data.

➢ RECORD WHAT HAPPENED

Helps IT identify the correct restore point and scope.

➢ CHECK RECYCLE BINS AND VERSION HISTORY

Often the fastest recovery path for cloud files.

➢ CONFIRM WHETHER BACKUPS ARE CLEAN

Avoids restoring corrupted or infected data.

➢ ESCALATE BEFORE EXPERIMENTING

Keeps a bad afternoon from becoming a permanent loss.

❖ ONGOING READINESS CHECKLIST

➢ MAINTAIN A DATA INVENTORY

You cannot protect data you cannot name or locate.

➢ BACK UP ENDPOINTS AND CLOUD SYSTEMS

Small-firm data often lives in both places.

➢ KEEP AN ISOLATED OR IMMUTABLE COPY

Protects against ransomware and administrator mistakes.

➢ SEPARATE BACKUP CREDENTIALS

Reduces the chance that one compromise destroys everything.

➢ MONITOR BACKUP ALERTS

Turns silent failures into fixable problems.

➢ TEST RESTORE PROCEDURES QUARTERLY

Proves that recovery works before a deadline depends on it.

- DOCUMENT RECOVERY CONTACTS AND KEYS

  Speeds response when the usual technology person is unavailable.

- REVIEW RETENTION WINDOWS ANNUALLY

  Cloud defaults and firm needs may not match.