

Essential Business Technology Policies (and Why They Matter)

Modern businesses operate in an environment where technology risk impacts revenue, reputation, and customer trust. Clear, well-maintained policies provide the structure teams need to operate safely, consistently, and in alignment with business goals. Organizations are best served by a streamlined, control-aligned policy framework that reduces duplication while meeting the expectations of cyber insurers, regulators, and widely adopted standards. This guide highlights the most impactful and common business technology policies expected by frameworks such as CIS Controls v8 (IG1), NIST Small Business Cybersecurity Guidance, and CISA Cyber Essentials.

Core Governance & Security Policies



Acceptable Use Policy (AUP)

Defines responsible use of company systems, networks, cloud applications, and data. Covers employee behavior, social media and public communications expectations, and user responsibilities related to phishing identification and reporting. Establishes baseline cyber hygiene and reduces accidental exposure. Can also include endpoint, mobile & BYOD guidance that establishes boundaries for personal device use. Addresses remote and hybrid work controls through device and identity requirements rather than separate telework rules.



Information Security Policy

Establishes the organization's overall security posture, roles, and baseline controls. Includes encryption and key-management requirements, security objectives, and alignment with recognized frameworks. Serves as the umbrella policy that technical standards support. May also address logging and monitoring, and additional layers of requirements for BYOD and remote workplaces.



Password, Authentication & MFA Policy

Sets requirements for password strength, credential protection, and multi-factor authentication. Critical for securing access to systems and required by most cyber insurance carriers.



Asset & Configuration Management Policy

Maintains an inventory of hardware, software, and cloud services and defines configuration standards. Foundational to all other security controls — you cannot protect what you do not know exists.



Access Control, Least Privilege & Account Change Policy

Defines how user access is requested, approved, reviewed, modified, and removed. Includes identity verification standards for account changes and password resets — a critical control for preventing social engineering attacks.



Vulnerability, Patch & Change Management Policy

Defines vulnerability scanning cadence, risk prioritization, patch timelines, and structured change approval. Reduces outages and minimizes exposure from unpatched systems and unauthorized changes.



Security Awareness & Training Policy

Defines required training topics, frequency, tracking, and accountability. Includes phishing simulations, reporting workflows, and reinforcement expectations. Essential for reducing human-driven risk.

Data Protection & Resilience



Data Classification, Handling, Retention & Destruction Policy

Defines data sensitivity levels and handling rules, along with retention schedules and secure destruction requirements. Includes media and device disposal controls to ensure sensitive data is properly sanitized or destroyed.



Backup, Recovery & Business Continuity Policy

Establishes recovery objectives, backup testing expectations, and continuity planning. Increasingly required by cyber insurers and critical for minimizing downtime during incidents.



Incident Response Policy & Plan

Defines roles, escalation paths, investigation steps, and response procedures. Includes breach-response communications, coordination with legal and insurers, and post-incident review.

Risk, Privacy & Third-Party Oversight



Privacy Policy & Privacy Program Controls

Defines how personal and sensitive data is collected, used, protected, and disclosed. Covers both public-facing privacy commitments and internal privacy governance controls.



Third-Party, Vendor & Cloud Risk Management Policy

Establishes due diligence, minimum security requirements, and ongoing oversight for vendors and cloud service providers. A major area of insurer and regulatory scrutiny.



Identity Theft Prevention (Red Flags) Policy

Required when “Covered Accounts” exist or when acting as a service provider. Defines detection, response, and prevention measures related to identity theft and misuse of personal data.

Practical Guidance for Making Policies Work

Tie policies to outcomes

Employees respond to uptime, customer trust, compliance — not technical jargon.

Assign clear ownership

Every policy needs a named owner. Policies fail when accountability defaults to “IT.”

Keep policies usable

Short, clear policies are far more effective than dense documents no one reads.

Review consistently

Annual review is a baseline. Revisit policies after incidents, audits, or major system changes.

Test what you document

Access reviews, incident response exercises, and backup tests often expose gaps.

Embed policies into onboarding

Employees should acknowledge essential policies such as Acceptable Use from day one.

Ground controls in CIS Controls

This provides a widely accepted baseline for essential cyber hygiene in SMB environments.

Next Steps

If your organization needs help drafting, consolidating, or maintaining these policies, Exigent’s Assurance Managed Services team can provide templates, best practices, and ongoing guidance. Through The Exigent Method, we help SMBs build practical, sustainable governance models that reduce risk and support long-term growth.