Net-Tech Compliance Policy Starter Kit

Purpose:

Provide the foundational set of written policies that establish your organization's baseline compliance posture and meet the "core control" requirements in the first 90 days.

Included Policies:

1. **Access Control Policy**
   - Define who can access systems, data, and applications.
   - Require strong passwords & MFA for all accounts.
   - Enforce least-privilege access.
2. **Incident Response Policy**
   - Define incident categories (e.g., ransomware, phishing, unauthorized access).
   - Establish reporting requirements and escalation steps.
   - Assign roles/responsibilities for incident response.
3. **Acceptable Use Policy (AUP)**
   - Define permitted and prohibited use of company systems, devices, and networks.
   - Address remote work security requirements.
   - Include disciplinary consequences for violations.
4. **Data Backup & Recovery Policy**
   - Define backup frequency, retention, and storage requirements.
   - Require regular recovery testing.
   - Document restoration procedures.
5. **Vendor Risk Management Policy**
   - Require vendor security assessments for any provider accessing sensitive data.
   - Maintain a vendor inventory and risk rating.

Implementation Tip: These policies should be **approved by leadership, distributed to all staff, and acknowledged in writing** (digital or physical signature) within the first 30 days.