Information Security Policy

Impact Risk Advisors

1. Policy Overview

This Information Security Policy outlines the security measures and responsibilities for protecting the information assets of Impact Risk Advisors. It is designed for small organizations with limited IT staff, relying on trusted cloud service providers such as Microsoft 365 and Google Workspace.

2. Policy Governance

Policy Owner: [Insert Role or Name]

Approver: [Insert Role or Name]

Review Date: [Insert Date]

Version: 1.0

This policy shall be reviewed at least annually or when significant changes occur.

3. Acceptable Use

Employees must use company systems, devices, and accounts responsibly. Activities such as unauthorized access, illegal downloads, and unapproved software installation are prohibited.

4. Access Control

Access to systems is granted on a least-privilege basis. All access must be approved and documented. MFA is required on all business-critical systems including Microsoft 365, VPN, and password managers.

5. Encryption

All data must be encrypted at rest and in transit. Reliance is placed on cloud providers (e.g., Microsoft 365, Google Workspace) to provide built-in encryption. Responsibility for configuration and user management remains with the organization.

6. Password & Authentication

Strong passwords and MFA are mandatory. A password manager must be used. Default configurations should be hardened where possible.

7. BYOD (Bring Your Own Device)

Personal devices used to access company data must have antivirus, disk encryption, and must not be shared with unauthorized individuals. Remote wipe must be enabled where possible.

8. Change Management / SDLC

For companies developing software, changes must be documented, tested, and reviewed before deployment. Version control systems and basic approval workflows (e.g., GitHub, Notion) are sufficient for small teams.

9. Security Awareness & Phishing

Employees must receive security awareness training at least annually. Simulated phishing tests should be conducted periodically using free or low-cost tools.

10. Physical Security

If operating from a physical office, access should be restricted to authorized personnel. Devices should be locked when unattended and visitors should sign in.

11. System Monitoring & Logs

Administrative and access logs from cloud services should be reviewed monthly. Alerts for suspicious activity should be enabled where supported by the platform.

12. Incident Response

All incidents must be documented and investigated. Impact Risk Advisors must have a basic response plan in place, including internal notification procedures and client communication if applicable.

Note: This section provides a high-level overview. A more detailed Incident Response Plan should be developed and maintained as a standalone document, outlining roles, response timelines, and containment procedures.

13. Vendor Management

Vendors with access to company data must be evaluated before onboarding. A simple vendor tracker should document services used and last review dates. SOC 2 reports or equivalent security documentation should be requested annually.

14. Data Retention & Disposal

Data retention schedules must align with legal and client requirements. Data should be securely deleted when no longer needed. Reliance on cloud provider deletion mechanisms is acceptable with validation.

15. Business Continuity & Disaster Recovery

Backup procedures must be documented and tested annually. Cloud platforms should have redundancy. Organizations must define a basic recovery plan.

Note: A detailed Disaster Recovery Plan (DRP) may be maintained as a standalone document, including RTOs, RPOs, recovery testing frequency, and contact lists.

16. System Security & Threat Management

All company endpoints must be protected by antivirus or endpoint detection and response (EDR) software. Definitions must be kept up to date and real-time protection enabled.

Vulnerability scans should be conducted monthly on company assets or cloud configurations, using internal or third-party tools. Critical vulnerabilities must be remediated in a timely manner.

If the organization develops and deploys software, third-party penetration testing should be conducted at least annually to identify application-level and infrastructure-level vulnerabilities. Documentation of remediation efforts should be retained.