Made by: Albin Axelsson, Founder of A Triple C Consulting (A3C) and Head of Business Development at GreenTally.ai

---

IT Risk Management Policy

Policy Number: P01

Document Owner: Management Board

Effective Date: [Insert Date]

Last Modified: [Insert Date]

Approved by: [Insert Approver Name]

Created by: [Insert Author Name]

Confidentiality: Internal

Table of Contents

---

1. Purpose

Define requirements for identifying, assessing, and treating IT risks to protect data integrity, confidentiality, and system availability. Focus on:

- Digital transformation risks (cloud, AI, automation)
- ESG/carbon data vulnerabilities
- Third-party platform dependencies

SME Implementation Tip: Start with critical systems first (e.g., financial/ESG data platforms).

2. Scope

Applies to:

- All hardware, software, SaaS, AI tools, and data assets
- Employees, contractors, and third parties handling IT/ESG systems

- New technology deployments (e.g., Greentally-style carbon tools)

Exclusions: Legacy systems scheduled for decommissioning within 6 months.

3. Policy Overview

3.1 Risk Management Process

Annual Enterprise Risk Assessment

- Use ISO 31000 or NIST SP 800-30 methodology
- Include AI model drift, cloud misconfigurations, and ESG data inaccuracies
- *Output:* Risk Register (Appendix A)

Risk Rating System

Rating	Criteria	Action Required
High (16-25)	Severe operational/financial impact	Mitigate within 30 days
Medium (6-15)	Moderate impact	Mitigate within 90 days
Low (1-5)	Minor impact	Monitor quarterly

Business Unit Reviews

- Quarterly self-assessments for teams using AI/cloud platforms
- Template: *"Has AI output validation failed in the last 90 days? [Y/N]"*

Annual IT Risk Report

Must include:

- Top 5 residual risks
- Insurance coverage gaps
- AI performance metrics

3.2 External Threat Management

Control	Frequency	Owner
Threat intel feeds (e.g., CISA)	Real-time	CISO
Industry ISAC participation	Quarterly	Risk Officer
Third-party platform audits	Bi-annual	Procurement

Threat Intel Checklist:

☐ Subscribe to ≥1 threat feed (e.g., InfraGard, sector-specific ISAC)

☐ Map threats to critical assets monthly

☐ Test incident response playbooks quarterly

3.3 Information Systems Risk

Pre-Deployment Analysis

For new tools (especially AI/ESG platforms):

1. Data lineage mapping
2. Bias testing (AI tools)
3. Failure scenario modeling

System Risk Reviews

- Production systems: Biannually
- AI models: Quarterly accuracy/drift checks
- High-risk changes: Pre-implementation review

3.4 Risk Treatment – Controls

Control Framework

Adopt one:

- ISO/IEC 27001
- NIST CSF
- COBIT

Material Risk Decisions

Option	Documentation Required
Accept	Board-signed waiver
Mitigate	Implementation plan with deadlines
Transfer	Insurance certificate

Ownership

- AI systems: Assign "Algorithm Custodian" role
- Cloud platforms: Designate "Configuration Steward"

3.5 Risk Treatment – Insurance

Coverage Requirements

Risk Type	Minimum Coverage
Cyber incidents	$1M per event
AI errors	$500K
Third-party failures	$2M

Annual Review Tasks:

☐ Validate BCP alignment

☐ Stress-test claim scenarios

☐ Benchmark against industry standards

3.6. Violations

Consequences:

- Tier 1 (Negligence): Mandatory retraining
- Tier 2 (Repeat/Systemic): Suspension + audit
- Tier 3 (Willful/Malicious): Termination + legal action

Reporting: Anonymized channel via [URL/email].

3.7 Definitions

Term	Definition
AI Platform	Algorithmic systems requiring bias/accuracy monitoring
ESG Data Risk	Inaccuracies in sustainability metrics affecting compliance
Residual Risk	Post-control risk quantified in annual report

3.8 References

- ISO 31000:2018 Risk Management
- NIST AI RMF (AI-specific controls)
- ENISA Cloud Security Guide

4. Risk Management Process

4.1 Overview

The organization will maintain a proactive, systematic approach to IT risk management, ensuring that all digital assets—including AI platforms and ESG data tools—are regularly assessed and protected. This process is designed to be scalable for SMEs and adaptable to new technologies.

4.2 Key Steps in the Risk Management Process

a. Risk Identification

- **Objective:** Catalog all potential threats to IT systems, data, and platforms (including AI/automation tools).
- **Actions:**
    - Inventory all digital assets (hardware, software, cloud, AI, ESG platforms).
    - Identify internal and external threats (e.g., cyberattacks, data breaches, AI model failures, third-party risks).
    - Engage with business units to surface operational risks.

b. Risk Assessment & Analysis

- **Objective:** Evaluate the likelihood and potential impact of identified risks.

- **Actions:**
    - Use a standardized risk matrix (e.g., 5x5 grid: Likelihood x Impact).
    - Assess vulnerabilities in systems, processes, and third-party integrations.
    - Analyze risks unique to AI (e.g., bias, drift, explainability issues).

c. Risk Evaluation & Prioritization

- **Objective:** Rank risks to focus on those with the greatest potential impact.
- **Actions:**
    - Assign risk ratings (High, Medium, Low) based on assessment results.
    - Prioritize risks that affect critical business operations, regulatory compliance, or ESG reporting.

d. Risk Treatment

- **Objective:** Determine and implement appropriate responses for each risk.
- **Actions:**
    - Choose to mitigate, transfer (e.g., insurance), accept, or avoid each risk.
    - Implement technical and organizational controls.
    - Assign ownership for risk mitigation actions.

e. Monitoring & Review

- **Objective:** Ensure risks are continuously managed and controls remain effective.
- **Actions:**
    - Schedule regular reviews (at least annually, or after major changes).
    - Monitor key risk indicators (KRIs), especially for AI and cloud platforms.
    - Update risk register and report changes to leadership.

f. Communication & Reporting

- **Objective:** Keep stakeholders informed and engaged.
- **Actions:**
    - Share risk assessment outcomes with relevant teams and management.
    - Document all risk management activities for audit and compliance.

4.3 Risk Management Process Checklist

Task	Frequency	Responsible Party	Status
Inventory all IT and digital assets	Annually / on acquisition	IT Manager	☐

Identify new and emerging threats (incl. AI/ESG)	Quarterly	Risk Officer	☐
Conduct formal risk assessment	Annually	Risk Committee	☐
Update risk register	After each assessment	Risk Officer	☐
Assign risk owners for all material risks	Ongoing	Management Board	☐
Review effectiveness of controls	Bi-annually	System Owners	☐
Test incident response procedures	Annually	IT Security Lead	☐
Report material risks to leadership	Annually / as needed	Risk Officer	☐
Re-assess risks after major changes (e.g., new AI tool)	As needed	Project Lead	☐

5. External Threat Sources

5.1 Overview

The organization recognizes that external threats—including cyberattacks, supply chain vulnerabilities, and emerging risks from third-party platforms and AI services—pose significant risks to IT and data integrity. This section outlines the approach to identifying, monitoring, and responding to these external threats.

5.2 Threat Intelligence

a. Subscriptions and Partnerships

- **Objective:** Maintain awareness of the latest cyber threats, vulnerabilities, and attack trends.
- **Actions:**
    - Subscribe to reputable threat intelligence feeds (e.g., national CERTs, sector-specific ISACs, commercial providers).
    - Establish information-sharing agreements with trusted industry partners.
    - Leverage vendor alerts for critical platforms and AI services.

b. Threat Analysis and Dissemination

- **Objective:** Analyze and communicate relevant threat information to stakeholders.
- **Actions:**
    - Regularly review threat intelligence for relevance to the organization's assets and platforms.
    - Disseminate actionable threat alerts to IT, security, and business unit leads.
    - Update risk assessments and controls in response to new threats.

5.3 Industry Collaboration

a. Participation in Security Networks

- **Objective:** Enhance collective defense through industry collaboration.
- **Actions:**
  - Participate in sector-specific cybersecurity forums and working groups.
  - Share anonymized incident data and best practices with peers.
  - Engage with regulatory and standards bodies on emerging risks (e.g., AI ethics, ESG data).

5.4 Third-Party and Supply Chain Risk

a. Vendor Risk Management

- **Objective:** Identify and manage risks originating from vendors, cloud providers, and AI service suppliers.
- **Actions:**
  - Maintain an up-to-date inventory of all third-party providers.
  - Conduct due diligence and periodic risk assessments for critical vendors.
  - Require contractual commitments for security standards and incident reporting.

b. Continuous Monitoring

- **Objective:** Detect and respond to changes in third-party risk posture.
- **Actions:**
  - Monitor vendor security bulletins and compliance certifications.
  - Implement automated tools for supply chain risk monitoring where feasible.
  - Reassess third-party risks after major incidents or service changes.

5.5 External Threat Sources Checklist

Task	Frequency	Responsible Party	Status
Subscribe to at least one threat intelligence feed	Annually	IT Security Lead	☐
Review and disseminate threat alerts	Monthly / As needed	Risk Officer	☐
Participate in industry security groups	Quarterly	CISO / Risk Officer	☐
Maintain inventory of third-party providers	Ongoing	Procurement	☐

Conduct vendor risk assessments	Annually	Procurement / IT Security	☐
Monitor vendor security updates	Ongoing	IT Security Lead	☐
Update risk register with new external threats	As needed	Risk Officer	☐
Reassess third-party risk after major incidents	As needed	Procurement / IT Security	☐

6. Information Systems Risk Management

6.1 Overview

Information systems—including core business platforms, cloud services, AI tools, and ESG/carbon data solutions—are critical to the organization's operations. This section defines how risks to these systems are proactively managed throughout their lifecycle, from planning and deployment to ongoing operation and decommissioning.

6.2 Pre-Deployment Risk Analysis

a. Impact Assessment

- **Objective:** Evaluate potential risks before introducing new systems or significant upgrades.
- **Actions:**
  - Conduct a formal risk assessment for all new information systems, with special attention to AI, cloud, and ESG platforms.
  - Assess data sensitivity, privacy implications, and regulatory requirements.
  - Identify dependencies and integration points with existing systems.

b. AI/Automation-Specific Considerations

- **Objective:** Address unique risks associated with AI/automation tools.
- **Actions:**
  - Test for algorithmic bias, explainability, and model drift.
  - Validate data sources and quality for AI/ESG applications.
  - Document fallback procedures in case of AI or automation failure.

6.3 Ongoing System Risk Reviews

a. Scheduled Reviews

- **Objective:** Ensure risks are continuously identified and managed during system operation.
- **Actions:**

- Conduct formal risk reviews of production systems at least every two years.
- For systems supporting critical processes or ESG data, conduct annual reviews.
- Review AI model performance and accuracy quarterly.

b. Change Management

- **Objective:** Control risks introduced by system changes.
- **Actions:**
  - Require risk assessments for all significant system changes, upgrades, or new integrations.
  - Update risk registers and controls after each change.

6.4 Incident Response Integration

a. Preparedness

- **Objective:** Ensure systems are ready to detect, respond to, and recover from incidents.
- **Actions:**
  - Integrate system monitoring with the organization's incident response plan.
  - Test incident response procedures for key systems annually.
  - Document lessons learned from incidents and update controls accordingly.

6.5 Information Systems Risk Management Checklist

Task	Frequency	Responsible Party	Status
Conduct risk assessment before new system deployment	As needed	Project Lead / IT Security	☐
Assess AI/automation tools for bias and explainability	Before deployment / Quarterly	Data Science Lead	☐
Review production system risks	Biannually	System Owner	☐
Review ESG/carbon data platform risks	Annually	ESG Data Owner	☐
Update risk register after system changes	As needed	Risk Officer	☐
Test incident response for key systems	Annually	IT Security Lead	☐
Document and review lessons learned from incidents	After each incident	System Owner	☐

6.6 SME Scalability Tips

- For smaller organizations, use a simple risk assessment template for all new systems.
- Focus on high-impact systems first (e.g., finance, ESG reporting).
- Schedule risk reviews during regular team meetings to streamline the process.

7. Risk Treatment – Controls

7.1 Overview

Risk treatment involves selecting and applying measures (controls) to reduce identified risks to acceptable levels. Controls may be technical, organizational, or procedural, and must be suitable for the organization's size, technology stack, and regulatory context.

7.2 Control Framework Adoption

a. Framework Selection

- **Objective:** Ensure a structured, best-practice approach to risk mitigation.
- **Actions:**
    - Adopt a recognized security framework (e.g., ISO/IEC 27001, NIST CSF, or COBIT).
    - Align controls with the organization's risk profile, including AI and ESG data considerations.
    - Regularly review framework relevance as technology and business needs evolve.

b. Customization for AI and ESG

- **Objective:** Address unique risks from AI platforms and ESG data systems.
- **Actions:**
    - Implement controls for AI model validation, monitoring, and explainability.
    - Ensure ESG data controls meet regulatory and reporting standards.
    - Require segregation of duties for sensitive data handling and model management.

7.3 Control Implementation

a. Control Types

- **Technical Controls:** Firewalls, encryption, access controls, monitoring, AI model validation tools.
- **Organizational Controls:** Policies, procedures, training, segregation of duties.
- **Physical Controls:** Secure server rooms, access badges, surveillance.

b. Assignment of Responsibilities

- **Objective:** Ensure clear accountability for control effectiveness.
- **Actions:**

- Assign control ownership to system owners, process leads, or designated "Control Stewards."
- Document responsibilities in the risk register or control matrix.
- Review and update assignments annually or after significant organizational changes.

7.4 Control Effectiveness and Review

a. Monitoring and Testing

- **Objective:** Verify that controls are operating as intended.
- **Actions:**
  - Perform regular control testing (e.g., penetration tests, vulnerability scans, AI output validation).
  - Review logs and monitoring reports for anomalies or control failures.
  - Update controls in response to new threats, incidents, or audit findings.

b. Continuous Improvement

- **Objective:** Adapt controls to evolving risks and technologies.
- **Actions:**
  - Solicit feedback from control owners and users.
  - Benchmark controls against industry standards and peer organizations.
  - Integrate lessons learned from incidents and audits.

7.5 Risk Treatment – Controls Checklist

Task	Frequency	Responsible Party	Status
Adopt and document security control framework	Annually / on framework update	IT Security Lead	☐
Implement technical, organizational, and physical controls	Ongoing	System Owners / IT	☐
Assign and review control ownership	Annually / on role change	Management Board	☐
Test technical controls (e.g., pen tests, AI validation)	Annually / after changes	IT Security Lead / Data Science Lead	☐
Review and update controls based on incidents/audits	After each event	Risk Officer	☐
Document control effectiveness in risk register	After each review	Risk Officer	☐

8. Risk Treatment – Insurance

8.1 Overview

Insurance is a key component of the organization's risk management strategy, providing financial protection against losses from IT, cyber, AI, and third-party incidents. This section outlines the approach to selecting, maintaining, and reviewing insurance coverage to address residual risks that cannot be fully mitigated by controls.

8.2 Insurance Coverage Guidelines

a. Coverage Requirements

- **Objective:** Ensure adequate financial protection for critical IT, cyber, and AI risks.
- **Actions:**
    - Maintain cyber liability insurance covering data breaches, ransomware, business interruption, and regulatory penalties.
    - Secure additional coverage for AI-specific risks (e.g., model errors, algorithmic failures, data bias incidents) if available.
    - Include third-party and supply chain risk coverage, especially for critical vendors and cloud/ESG platforms.

b. Alignment with Business Continuity Planning (BCP)

- **Objective:** Ensure insurance supports recovery from major incidents and aligns with BCP.
- **Actions:**
    - Review insurance policies to confirm alignment with BCP scenarios (e.g., extended outages, data loss, ESG reporting failures).
    - Ensure insurance covers costs associated with business restoration, data recovery, and regulatory reporting.

c. Documentation and Claims Management

- **Objective:** Facilitate efficient claims processing and compliance.
- **Actions:**
    - Maintain up-to-date records of all insurance policies, coverage limits, and exclusions.
    - Assign responsibility for insurance management to a designated officer.
    - Document all claims and outcomes for audit and continuous improvement.

8.3 Annual Insurance Review

- **Objective:** Ensure insurance remains appropriate for the organization's evolving risk profile.
- **Actions:**
  - Conduct an annual review of all insurance policies with input from IT, risk, and finance teams.
  - Benchmark coverage against industry standards and peer organizations.
  - Adjust coverage levels and terms based on changes in technology, business operations, or regulatory requirements.

8.4 Risk Treatment – Insurance Checklist

Task	Frequency	Responsible Party	Status
Maintain cyber liability insurance	Ongoing	Finance / Risk Officer	☐
Review and update insurance for AI/ESG risks	Annually	Risk Officer / IT	☐
Ensure insurance aligns with BCP scenarios	Annually	Risk Officer / BCP Lead	☐
Document all insurance policies and claims	Ongoing	Finance	☐
Conduct annual insurance adequacy review	Annually	Senior Leadership	☐
Benchmark insurance coverage against peers	Annually	Risk Officer	☐
Update risk register with insurance details	Annually / after changes	Risk Officer	☐

9. Violations

9.1 Overview

Adherence to the IT Risk Management Policy is mandatory for all employees, contractors, and third parties. Non-compliance undermines the organization's ability to manage risk and may result in operational, financial, or reputational harm.

9.2 Reporting Violations

a. Reporting Mechanisms

- **Objective:** Encourage prompt reporting of policy breaches or suspected non-compliance.
- **Actions:**
  - Provide clear channels for reporting violations (e.g., dedicated email, hotline, or anonymous web form).
  - Ensure all reports are treated confidentially and investigated promptly.
  - Protect whistleblowers from retaliation.

b. Escalation Procedures

- **Objective:** Ensure serious or repeated violations are escalated appropriately.
- **Actions:**
    - Minor violations handled by line managers or HR.
    - Serious or systemic violations escalated to senior management or the board.
    - Legal counsel engaged for breaches involving regulatory or contractual obligations.

9.3 Consequences of Violations

- **Tier 1 (Minor/First Offense):**
    - Retraining and documented warning.
- **Tier 2 (Repeat/Moderate Offense):**
    - Temporary suspension of system access, formal investigation, and performance review.
- **Tier 3 (Severe/Willful Breach):**
    - Termination of employment or contract, and potential legal action.
- **Third-Party Violations:**
    - May result in contract termination or legal claims.

9.4 Documentation and Remediation

- **Objective:** Ensure all violations are logged, investigated, and remediated.
- **Actions:**
    - Maintain a violation log with details of incidents, investigations, and outcomes.
    - Document corrective actions and lessons learned.
    - Update risk assessments and controls to prevent recurrence.

9.5 Violations Enforcement Checklist

Task	Frequency	Responsible Party	Status
Provide and publicize reporting channels	Ongoing	HR / Risk Officer	☐
Investigate reported violations promptly	As needed	HR / IT Security	☐
Escalate serious violations per procedure	As needed	HR / Management	☐
Document all violations and outcomes	Ongoing	Risk Officer	☐
Apply disciplinary measures consistently	As needed	HR / Management	☐
Update controls based on lessons learned	After each incident	IT Security / Risk Officer	☐

10. Definitions

10.1 Key Terms

Term	Definition
Information Asset	Any data, system, application, platform, or digital tool used in business operations or decision-making.
Risk	The likelihood that a threat will exploit a vulnerability, resulting in adverse impact on confidentiality, integrity, or availability.
Threat	Any circumstance or event with the potential to cause harm to information systems, data, or operations.
Vulnerability	A weakness in systems, processes, or controls that can be exploited by threats.
Residual Risk	The level of risk remaining after controls and mitigation measures have been applied.
Control	A safeguard or countermeasure (technical, organizational, or physical) implemented to reduce risk.
AI Platform	Software or system that uses machine learning or artificial intelligence to automate or enhance business processes.
Model Drift	The degradation of an AI model's performance over time due to changes in data or environment.
ESG Data	Environmental, Social, and Governance data, including carbon metrics and sustainability reporting information.
Incident	An event that compromises the confidentiality, integrity, or availability of information assets.
Risk Register	A documented record of identified risks, their assessments, owners, and treatment actions.
Business Continuity Planning (BCP)	The process of preparing for, responding to, and recovering from disruptive incidents to ensure ongoing operations.
Third-Party Risk	Risks arising from vendors, suppliers, contractors, or service providers who access or process organizational data.
Control Steward	The individual assigned responsibility for implementing and maintaining a specific control.
Algorithm Custodian	The individual responsible for the oversight, validation, and performance monitoring of an AI model or platform.

11. References

11.1 Standards and Frameworks

Reference	Description	Applicability
ISO/IEC 27001	International standard for information security management systems (ISMS).	Security controls, risk process

ISO/IEC 27002	Code of practice for information security controls.	Control implementation
ISO 31000	International standard for risk management principles and guidelines.	Enterprise risk management
NIST SP 800-30	Guide for conducting risk assessments (National Institute of Standards and Technology).	Risk assessment methodology
NIST Cybersecurity Framework	Voluntary framework for improving cybersecurity risk management.	Control selection, maturity
NIST AI RMF	Risk Management Framework for Artificial Intelligence.	AI-specific risk management
ENISA Cloud Security Guide	Guidance from the European Union Agency for Cybersecurity on securing cloud services.	Cloud and SaaS risks
PCI DSS	Payment Card Industry Data Security Standard; annual risk assessment requirements.	Payment and data security

11.2 Regulatory and Industry Resources

Reference	Description
GDPR	General Data Protection Regulation (EU data privacy law).
DORA	Digital Operational Resilience Act (EU financial sector).
CISA Alerts	Cybersecurity & Infrastructure Security Agency threat intelligence.
Sector-specific ISACs	Information Sharing and Analysis Centers for industry threat sharing.

11.3 Internal Documents

Document Name	Purpose
P01-001: Information Security Policy	Overall information security governance
P01-006: AI Procurement Guidelines	Guidance for acquiring and integrating AI tools
P01-007: Third-Party Risk Standard	Vendor and supply chain risk management
Business Continuity Plan (BCP)	Recovery and resilience planning

12. Training Needs

12.1 Overview

To maintain an effective IT risk management posture, all personnel must understand their roles, responsibilities, and the procedures outlined in this policy. Training ensures that staff can identify, report, and respond to IT risks, especially those related to emerging technologies such as AI and ESG data platforms.

12.2 Training Requirements by Role

Role/Function	Training Requirement	Frequency

All Employees	Awareness of IT Risk Management Policy and reporting channels	Onboarding, Annually
IT & System Owners	In-depth training on control frameworks, risk assessment, and incident response	Annually
AI Users/Developers	Training on AI risk (bias, drift, explainability), model validation, and ethical use	Annually, or on major updates
ESG Data Owners	Training on ESG data integrity, regulatory requirements, and system risk controls	Annually
Third-Party Managers	Vendor risk management and supply chain security	Annually
Executives/Board	Overview of risk management responsibilities and reporting obligations	Annually

12.3 Training Delivery Methods

- **E-learning modules:** For general awareness and policy updates.
- **Workshops/Seminars:** For specialized roles (e.g., AI, ESG, IT).
- **Tabletop exercises:** For incident response and risk scenario testing.
- **Quizzes/Assessments:** To verify understanding and retention.

12.4 Training Records and Compliance

- Maintain a central log of all completed training and attendance.
- Require annual attestation of policy understanding for all staff.
- Review training content and participation annually to ensure relevance and completeness.

12.5 Training Needs Checklist

Task	Frequency	Responsible Party	Status
Update training materials to reflect policy changes	As needed	HR / IT Security	☐
Deliver onboarding and annual refresher training	Ongoing/Annually	HR / Department Leads	☐
Conduct role-specific workshops and exercises	Annually	IT / Risk Officer	☐
Track and document all training completions	Ongoing	HR	☐
Review and improve training content	Annually	HR / Risk Officer	☐

13. Related Documents

13.1 Internal Policies and Standards

Document Name	Description/Scope	Owner/Department
P01-001: Information Security Policy	Establishes overall information security governance, roles, and responsibilities.	IT / Risk Management

P01-006: AI Procurement Guidelines	Outlines requirements and best practices for acquiring, validating, and integrating AI solutions.	Procurement / IT
P01-007: Third-Party Risk Standard	Sets standards for vendor selection, risk assessment, and ongoing monitoring.	Procurement / Risk
Business Continuity Plan (BCP)	Details procedures for maintaining operations during and after disruptive incidents.	Operations / BCP Lead
Incident Response Plan	Provides step-by-step guidance for detecting, reporting, and managing IT security incidents.	IT Security
Data Privacy Policy	Defines rules for handling personal and sensitive data in compliance with applicable regulations.	Legal / Compliance
Digital Tools & Platform Governance Policy (Optional)	Sets governance standards for the adoption and management of digital and cloud platforms.	IT / Digital Strategy
AI Use and Ethics Policy (Optional)	Establishes principles and controls for responsible AI use and monitoring.	AI Governance / Ethics

13.2 Document Management

- **Access:** All related documents must be readily accessible to relevant staff via the organization's document management system or intranet.
- **Review:** Related documents should be reviewed and updated in alignment with this policy's review cycle or when significant changes occur.
- **Cross-Reference:** Where applicable, this policy should reference and align with the requirements and controls set out in related documents to ensure consistency.

14. Appendices

Appendix A: Risk Register Template

A structured template for documenting, tracking, and managing identified IT risks.

Risk ID	Description	Impact	Likelihood	Risk Rating	Owner	Treatment Action	Status	Review Date
001	Example: Cloud outage	High	Medium	High	IT Manager	Mitigate	Open	2025-07-01
002	Example: AI model drift	Medium	Medium	Medium	Data Scientist	Monitor	Open	2025-07-01

Appendix B: Implementation Checklist

A comprehensive checklist to ensure all policy requirements are addressed and regularly reviewed.

Task	Frequency	Responsible Party	Status

Complete annual risk assessment	Annually	Risk Officer	☐
Validate AI tools for bias and accuracy	Quarterly	Data Science Lead	☐
Review insurance coverage for IT and AI risks	Annually	Finance/Risk Officer	☐
Update risk register after system or process changes	As needed	Risk Officer	☐
Conduct incident response exercises	Annually	IT Security Lead	☐
Deliver staff training on IT risk and policy changes	Annually/As needed	HR/IT	☐
Review and update controls based on incidents/audits	After each event	IT Security/Risk	☐

Appendix C: SME Quick-Start Guide

A simplified roadmap for small and medium-sized enterprises to implement core elements of the policy efficiently.

1. **Identify Critical Systems:** List your most important digital assets (e.g., finance, ESG, cloud platforms).
2. **Assess Key Risks:** Use the risk register template to document top 5 risks.
3. **Apply Basic Controls:** Implement strong passwords, enable MFA, and schedule regular backups.
4. **Assign Ownership:** Designate a responsible person for each key system and risk.
5. **Schedule Reviews:** Hold quarterly check-ins to update risks and controls.
6. **Train Staff:** Provide a short annual briefing on IT risks and reporting procedures.
7. **Document Everything:** Keep records simple and accessible (spreadsheet or shared folder).

Appendix D: Training Tracker Template

A tool for tracking completion and compliance with training requirements.

Employee Name	Role	Training Completed	Date	Next Due	Comments
Jane Smith	IT Manager	Yes	2025-05-15	2026-05	Refresher needed
John Doe	Data Analyst	Yes	2025-03-20	2026-03	

Appendix E: Incident Log Template

A template for logging and tracking IT security incidents and responses.

Incident ID	Date	Description	Impact	Actions Taken	Status	Lessons Learned
INC-2025-01	2025-04-10	Phishing attempt	Low	Blocked sender	Closed	Staff training

Appendix F: Policy Review & Signoff

- **Review Cycle:** Annually, or after major changes in technology, business operations, or regulations.

- **Approval:**
  - [Name/Date] – Management Board
  - [Name/Date] – IT Director

At **GreenTally.ai**, our mission is to empower companies like yours to take the first step with confidence.

Contact us at Ning@greentally.ai / Albin@greentally.ai

Let's explore what ESG can really mean for your bottom line.