## **ISO 27001 Email Policy Template**

### **1. Introduction**

This document outlines the Email Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes guidelines for the secure and appropriate use of the organization’s email systems to protect information and reduce risks.

### **2. Purpose**

The purpose of this policy is to:

1. Define acceptable use of email systems to safeguard organizational information.
2. Mitigate risks associated with email misuse, such as phishing attacks and data leaks.
3. Establish roles and responsibilities for email use and administration.

### **3. Scope**

This policy applies to all employees, contractors, and third-party users with access to [Organization Name]’s email systems. It includes:

* Internal and external email communications.
* Use of personal email accounts for work purposes, permitted only with prior written approval from management and in compliance with organizational security guidelines.

### **4. Policy Statement**

[Organization Name] commits to ensuring that email systems are used securely, professionally, and in alignment with ISO 27001 standards. This includes:

1. Ensuring email systems are protected against unauthorized access and threats.
2. Using email systems solely for legitimate business purposes.
3. Prohibiting activities that compromise security or violate organizational policies, such as sending unencrypted sensitive information, clicking on suspicious links, or using email systems for personal commercial purposes.

### **5. Roles and Responsibilities**

1. **Email Users:** Adhere to acceptable use guidelines, report suspicious activities, and safeguard their credentials.
2. **IT Department:** Manage and secure email systems, monitor usage, and enforce this policy.
3. **Information Security Officer (ISO):** Ensure compliance with ISO 27001 and oversee email security measures.

### **6. Compliance and Monitoring**

1. Use automated tools, such as Proofpoint, Mimecast, or Microsoft Defender for Office 365, to monitor email systems for phishing attempts, unauthorized access, or suspicious attachments.
2. Conduct regular audits to ensure adherence to this policy.
3. Enforce disciplinary measures for violations of this policy.

### **7. Related Documentation**

1. Acceptable Use Policy
2. Information Security Policy
3. Incident Management Policy

### **8. Review and Revision**

This policy will be reviewed annually or when significant changes occur in email systems or applicable regulations. Updates will be coordinated by the Information Security Officer.

### **Appendix A: Acceptable Use Guidelines**

| **Use Case** | **Guidelines** | **Notes** |
| --- | --- | --- |
| Business Emails | Use for legitimate business purposes only. |  |
| External Emails | Encrypt sensitive information before sending. |  |

### **Appendix B: Email Incident Report Template**

| Incident ID | Date/Time | Description of Incident | Actions Taken | Resolution Status |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

### **Appendix C: Policy Acknowledgment Form**

I acknowledge that I have read and understood the Email Policy and agree to comply with its requirements.

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_