

Human Resources Policies at Electric Inc.

Introduction

Electric Inc. is committed to fostering a workplace that balances employee well-being, data integrity, and organizational confidentiality. This overview summarizes three cornerstone HR policies—Holiday & Leave, Data Security, and Confidentiality & Non-Disclosure—that all employees must understand and follow. These policies ensure fair treatment, protect sensitive information, and uphold Electric Inc.'s reputation for integrity.

1. Holiday & Leave Policy

1.1 Annual Leave Entitlement

- **Full-Time Employees:** Accrue 20 days of paid annual leave per calendar year, prorated in the first year of service.
- **Part-Time Employees:** Accrue leave on a pro-rata basis relative to hours worked.
- **Accrual Schedule:** Leave accrual begins on the first day of employment and is credited monthly (1.67 days per month).

1.2 Public Holidays

- Electric Inc. observes all national statutory holidays in each country of operation.
- If a public holiday falls on a weekend, the following business day is observed.

1.3 Leave Scheduling & Approval

- **Request Window:** Employees should submit leave requests at least four weeks before planned time off.
- **Approval Process:**
 1. Submit requests via the HR portal.
 2. Line managers review operational needs and staffing levels.
 3. Employees receive approval or denial within five business days.
- **Blackout Periods:** During peak business cycles (e.g., year-end close), leave requests may be limited or postponed to ensure coverage.

1.4 Carryover & Payout

- **Carryover Limit:** Up to 5 unused days may be carried forward into the next calendar year; any excess is forfeited unless otherwise approved by HR.
- **Payout:** Upon termination, employees receive payment for unused accrued leave at the final base salary rate.

1.5 Special Leave Types

- **Sick Leave:** 10 days of paid sick leave per year; requires a doctor's note for absences exceeding three consecutive days.

- **Parental & Compassionate Leave:** As per local regulations, employees may be eligible for maternity, paternity, or compassionate leave; details and application forms are available on the HR intranet.
-

2. Data Security Policy

2.1 Purpose & Scope

This policy governs the handling, storage, and transmission of Electric Inc.'s digital and physical information assets. It applies to all employees, contractors, and third-party vendors with access to company systems.

2.2 Employee Responsibilities

- **Data Classification:** Identify and label information as *Public*, *Internal*, or *Confidential* based on sensitivity.
- **Access Control:**
 - Use unique user IDs and strong passwords (minimum 12 characters, including uppercase, lowercase, digits, and symbols).
 - Enable multi-factor authentication (MFA) on all critical systems.
- **Device Security:**
 - Lock screens when unattended.
 - Encrypt laptops and mobile devices.
 - Install only approved software and keep systems patched.

2.3 Acceptable Use & Network Security

- **Email & Internet:**
 - Do not click on suspicious links or open unknown attachments.
 - Forward phishing attempts to IT Security immediately.
- **Remote Access:**
 - Connect only via the company's VPN.
 - Ensure home networks meet basic security standards (updated router firmware, strong Wi-Fi passwords).

2.4 Incident Reporting & Response

- **Reporting:** All actual or suspected security incidents (breaches, lost devices, unauthorized access) must be reported to the IT Security team within 2 hours.
- **Response:** The Security Incident Response Team (SIRT) will classify, contain, and remediate incidents according to the Incident Response Plan.

2.5 Training & Compliance

- **Annual Training:** Employees must complete a mandatory Data Security Awareness course each year.
 - **Audits:** Periodic internal and external audits verify compliance; non-compliance may result in disciplinary action up to termination.
-

3. Confidentiality & Non-Disclosure Policy

3.1 Definitions

- **Confidential Information:** Any non-public business, technical, financial, or customer data that Electric Inc. deems proprietary.
- **Third-Party Confidential Data:** Information belonging to customers, partners, or suppliers under contractual confidentiality obligations.

3.2 Non-Disclosure Obligations

- **NDA Requirement:** All employees sign a standard Non-Disclosure Agreement (NDA) on or before their first day.
- **Scope of NDA:**
 - Survives employment and extends for 3 years after separation.
 - Covers oral, written, and electronic disclosures.

3.3 Permitted Disclosures

- **Internal Sharing:** Employees may share confidential information on a *need-to-know* basis within the company.
- **External Disclosures:** Must have prior written approval from Legal or designated senior management. Public disclosures (e.g., press releases) follow the Corporate Communications protocol.

3.4 Protection & Secure Handling

- **Physical Documents:**
 - Store in locked cabinets when not in use.
 - Shred all confidential paper before disposal.
- **Digital Documents:**
 - Store in encrypted folders on the company network or approved cloud services.
 - Do not transfer via personal email or unauthorized file-sharing tools.

3.5 Violations & Consequences

- **Investigation:** Alleged breaches are investigated by HR and Legal.
- **Disciplinary Action:** May include written warnings, forfeiture of bonuses, or termination.
- **Legal Remedies:** Electric Inc. reserves the right to pursue injunctive relief and damages for any unauthorized disclosure.

Conclusion

Electric Inc.'s HR policies strike a balance between employee flexibility, robust data protection, and strict confidentiality. Adherence to these guidelines helps maintain a supportive work environment, safeguards proprietary and customer information, and upholds our ethical standards. For full policy details, forms, and procedure guides, please refer to the HR portal and the Employee Handbook or contact the HR team directly.