IT & Security Coordinator

About NatureFinance

NatureFinance is a Swiss-based, international non-profit organization dedicated to aligning global finance with more equitable, nature positive outcomes. We work to make nature count in global finance and the global economy. NatureFinance is active in advancing the use of data to disclose and manage nature related risks, developing impactful and equitable nature markets, and advancing financial innovation in the areas of sovereign debt and nature positive investment. We develop tools to help financial actors better assess and align their investments with nature positive outcomes and push for stronger costs and consequences where finance is failing to address nature liabilities. We work remotely and pride ourselves on a collaborative and supportive work environment.

Role overview

The **IT & Security Coordinato**r is a pivotal role that combines the responsibilities of both Technology Security Coordinator and Information Security Coordinator. This position is responsible for ensuring the security of the organization's technology infrastructure and the protection of its information assets and websites. The role involves developing and implementing comprehensive IT security policies, managing IT security systems, conducting risk assessments, ensuring compliance with relevant regulations and liaising with external IT providers. The IT & Security Coordinator also leads IT incident response efforts and promotes IT security awareness across the organization.

This role requires a proactive approach to anticipate potential IT security challenges and implement measures that minimize risk to the organization. The IT & Security Coordinator plays a crucial part in maintaining a secure environment that enables the organization to operate efficiently and without disruption.

Key Responsibilities

Policy Development and Implementation

- Develop and enforce IT security policies, procedures, and protocols.
- Regularly review and update IT security policies to ensure compliance and effectiveness.

Risk Management and Assessment

- Conduct risk assessments to identify potential IT security threats.

- Perform regular IT security audits to ensure compliance and identify areas for improvement.

IT Security Systems Management

- Oversee the installation, maintenance, and operation of security systems (e.g., firewalls, intrusion detection systems, antivirus software).
- Monitor and respond to IT security incidents, compiling detailed reports.

IT Incident Response and Management

- Develop and implement IT incident response plans for security breaches and cyber-attacks.
- Lead the response to IT security incidents, ensuring timely and effective resolution.

Compliance and Regulatory Adherence

- Ensure compliance with security frameworks and regulations such as ISO 27001 and GDPR.
- Coordinate and prepare for external IT security audits and assessments.

IT Security Awareness and Training

- Conduct training programs for staff on IT security best practices and policies.
- Develop and distribute materials to promote IT security awareness throughout the organization.

Coordination and Communication

- Liaise with law enforcement and emergency responders during IT security incidents.
- Collaborate with various departments to ensure comprehensive IT security coverage and address specific IT security needs.

Website Security Oversight

- Regularly monitor the security of all company websites (3- 5 websites) to identify and mitigate potential vulnerabilities.
- Ensure that appropriate IT security measures, and regular security patches, are in place and maintained

Liaison with External IT Providers and Consultants

- Work closely with external IT security providers and consultants to ensure the security of the organization's websites and data.
- Assess and manage risks associated with third-party vendors and service providers, ensuring they adhere to the organization's IT security policies and procedures.

Qualifications and Experience

Education:

- Bachelor's degree in information security, Cybersecurity, Computer Science, or a related field.
- Strong knowledge of network security, risk management, and compliance frameworks.
- Microsoft 365 certification is required.
- Relevant certifications such as CISSP, CISM, or CEH are a plus.
- Proficiency in English.

Experience:

- At least 3-5 years of experience in IT security operations, including managing security systems and responding to IT security incidents.
- Proven experience in developing and implementing IT incident response plans, and effectively managing IT security incidents.
- Excellent communication skills to effectively convey IT security policies and procedures to NF Team members.
- Experience in writing detailed reports on IT security incidents and risk assessments.
- Experience in startups space and non for profits is desirable

Technical Skills:

- Risk Assessment: Ability to identify, analyze, and evaluate potential risks to the organization's assets and operations.
- Incident Response: Proficiency in developing and implementing IT incident response plans, and effectively managing security incidents .
- Network Security: Knowledge of network security principles, including firewalls, intrusion detection systems, and antivirus software.
- Cybersecurity Frameworks: Familiarity with cybersecurity frameworks and standards such as ISO 27001, NIST, and GDPR2.
- Vulnerability Management: Skills in identifying and mitigating vulnerabilities in IT systems.
- Security Information and Event Management (SIEM): Experience with SIEM tools to monitor and analyze security events

Analytical Skills

- Risk Analysis: Ability to assess the likelihood and impact of identified threats.
- IT Security Audits: Conducting regular IT security audits to ensure compliance and identify areas for improvement.
- Threat Intelligence: Gathering and analyzing threat intelligence to stay ahead of potential IT security threats.

Soft Skills

- Communication: Excellent verbal and written communication skills to effectively convey IT security policies and procedures to NF Team Members

- Leadership: Proven ability to lead and manage IT security operations, including coordinating with various departments and external providers.
- Problem-Solving: Strong problem-solving skills to address IT security incidents and vulnerabilities quickly and effectively.
- Attention to Detail: Keen attention to detail to identify potential IT security risks and ensure thorough implementation of security measures.
- Collaboration: Ability to work collaboratively with different departments to ensure comprehensive security coverage
- Training and Awareness: Skills in conducting training programs and promoting IT security awareness throughout the organization.

Personal Attributes:

- **Cultural Sensitivity:** Understanding and respect for diverse cultural perspectives, especially in the context of working with different geographies, cultures and backgrounds.
- **Adaptability:** Flexibility to adapt to changing priorities and work environments.
- **Integrity:** High ethical standards and a commitment to confidentiality and professionalism.
- **Initiative**: Self-motivated with a proactive approach to work and the ability to drive initiatives independently.

Terms

The role will be full-time, working remotely, with a preference for a candidate located within Europe, or at least within GMT/CET time zone.

The team member notes that, due to the characteristics of the Foundation's business and the position, they might be required to do some trips. The Foundation can determine the means of transport. The gross salary will not be affected by this, and the Foundation will either supplies cash in advance or reimbursed in full all costs associated to the business travels including but not limited to flights, hotel, and other expenses associated with the business trip.

This job description outlines the primary responsibilities and requirements for the IT & Security Operations Coordinator at NatureFinance. The IT & Security Coordinator may be requested to undertake additional activities to support the NatureFinance team, as per the Finance & Operations Director request. This role requires flexibility and a collaborative approach to ensure the smooth functioning of NF operations.

NatureFinance is an Equal Opportunity Employer

We are committed to fostering a diverse and inclusive workforce and encourage candidates from all backgrounds to apply. We look forward to welcoming a dynamic individual who shares our passion for aligning finance with nature-positive outcomes.

How to Apply:

Interested candidates are invited to submit their resume and a cover letter detailing their qualifications and experience related to this position's requirements. Applications should be sent to operations@naturefinance.net by 30th August.

Please note that due to the high volume of applications we receive, NF may not be able to respond to every applicant. Only candidates selected for further consideration will be contacted.