

<https://www.iconnectitbs.com/careers/security-engineer-remote/>

## Description

We are seeking a highly skilled Email Security and Compliance Engineer to join our team. In this role, you will be responsible for ensuring the security, integrity, and compliance of our email infrastructure. You will implement and maintain security measures, manage email backups and archives, conduct awareness training, and oversee DMARC implementation.

## Hiring organization

iConnect IT Business Solutions

## Date posted

November 11, 2024

## Responsibilities

- **Email Security:**
  - Implement and manage email security solutions, including spam filters, antivirus, and intrusion detection systems.
  - Monitor for and respond to email-borne threats, such as phishing attacks, malware, and ransomware.
  - Conduct regular security assessments and vulnerability scans.
  - Stay informed about emerging email security threats and trends.
- **Email Backup and Archiving:**
  - Implement and maintain robust email backup and archiving solutions.
  - Ensure compliance with data retention and regulatory requirements.
  - Restore lost or corrupted emails as needed.
- **Email Awareness Training:**
  - Develop and deliver effective email security awareness training programs for employees.
  - Educate users about phishing attacks, social engineering, and other email-related threats.
  - Promote best practices for email security hygiene.
- **DMARC Management:**
  - Implement and manage DMARC policies to authenticate email and prevent spoofing.
  - Monitor DMARC reports and take corrective action to address issues.
  - Work with DNS providers to configure DMARC records.
- **Email Compliance:**
  - Ensure compliance with relevant email security and privacy regulations (e.g., GDPR, CCPA, HIPAA).
  - Conduct regular audits and assessments to identify and mitigate compliance risks.

## Qualifications

- Strong understanding of email security principles and best practices.
- Experience with email security solutions (e.g., Proofpoint, Mimecast, Barracuda).
- Knowledge of email protocols (SMTP, IMAP, POP3).
- Proficiency in scripting and automation tools (e.g., PowerShell, Python).
- Excellent troubleshooting and problem-solving skills.
- Strong written and verbal communication skills.
- Ability to work independently and as part of a team.
- Certifications in email security or cybersecurity.

- Experience with cloud-based email security solutions.
- Knowledge of SIEM and log analysis tools.