## Information Security Analyst Job Description

Information security analysts design, implement, monitor, and evaluate the security systems that protect an organization’s computer systems and data. Add your information security analyst roles and responsibilities to our information security analyst description to begin creating a detailed, professional job listing for your business.

We are hiring an Information Security Analyst to work in our growing IT Security team. You will monitor our computer networks for security issues, install security software, and document any security issues or breaches you find. To do well in this role you should have a bachelor's degree in computer science and experience in the information security field.

### Information Security Analyst Responsibilities:

* Monitor computer networks for security issues.
* Investigate security breaches and other cyber security incidents.
* Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs.
* Document security breaches and assess the damage they cause.
* Work with security team to perform tests and uncover network vulnerabilities.
* Fix detected vulnerabilities to maintain a high-security standard.
* Stay current on IT security trends and news.
* Develop company-wide best practices for IT security.
* Perform penetration testing.
* Help colleagues install security software and understand information security management.
* Research security enhancements and make recommendations to management.
* Stay up-to-date on information technology trends and security standards.

### Information Security Analyst Requirements:

* Bachelor's degree in computer science or related field.
* MBA in information systems.
* Experience in information security or related field.
* Experience with computer network penetration testing and techniques.
* Understanding of firewalls, proxies, SIEM, antivirus, and IDPS concepts.
* Ability to identify and mitigate network vulnerabilities and explain how to avoid them.
* Understanding of patch management with the ability to deploy patches in a timely manner while understanding business impact.