# Security Administrator  1

## Job summary

We're seeking a <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> with a strong background in security protocols, infrastructure hardening, and PowerShell. This role would identify the severity of reported issues and gather appropriate documentation to identify root causes. This role would work collaboratively with software vendors and Spectrio personnel to resolve issues.

## Responsibilities

Installs, administers, and troubleshoot customers security solutions

Troubleshoot any access problems and implement network security policies and application security, access control and corporate data safeguards and monitor patch management to ensure network equipment and operating systems are protected against vulnerabilities

Ensure the network's security, protection against unauthorized access, modification, or destruction

Configuring and supporting security tools such as anti-virus software and patch management systems

Scanning and assessing network for vulnerabilities

Monitoring network traffic for unusual activity

Implementation of email security standards such as DKIM, SPF and DMARC

Maintain email security infrastructure, providing stability by developing tools, policies, processes, and procedures for the operations teams

Provide a secure environment, by implementing controls to manage and mitigate risks

Develop automated metrics reporting capabilities

Create, review, maintain and update documentation including Documenting ITGlue

Work with colleagues to provide consistent processes and solutions and Implement network security policies, application security, access control and corporate data safeguards

Investigate & Troubleshoot root causes when escalated from operations

Escalate and liaise with additional internal/external groups when required

Developing and updating business continuity and disaster recovery protocols

## Requirements

Excellent Communication Skills (written and verbal).

1-2 years of experience (Help Desk, IT)

Passionate about technology and networking, and able to learn and develop independently

Customer service-driven attitude – Awesomeness!

Must be “proactive” whenever possible – this includes monitoring and self-assigning tasks

Willingness to travel, if required.

Task Management and Administration Discipline – Administrators are accountable for the proper administration of “assigned” Tasks including documentation, proper closure including root cause analysis, incident profiling, tagging, and appropriate escalation

Communicates effectively with clients to identify needs and evaluate alternative business solutions with company project management

Continually seeks opportunities to increase internal client satisfaction and deepen client relationships

Manages client expectations effectively

# Security Administrator  2

## Job summary

The <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> is responsible for assisting the <a href="https://100hires.com/security-architect-job-description.html">security architect</a> in implementing, configuring, and supporting the various organizational tools needed to protect enterprise information. Ensuring stated corporate security policies are enforced upon a reliable 24x7 production environment. Comprehension of critical security concepts and how to develop and implement secure procedures according to developed policy. Analysis of key metrics is used to determine the availability and effectiveness of design/equipment configuration. This can and frequently does include system configuration level changes (on key mission-critical supporting components) as well as risk-mitigating devices. Incumbents must be quick and efficient in dealing with a heavy and diversified work processing load. Excellent Customer Service is a priority.

## Responsibilities

Assist the <a href="https://100hires.com/security-architect-job-description.html">security architect</a> in leveraging available tools, contracted security partners, and available resources to identify security threats to the organization and create steps to defend against them.

Incumbent must demonstrate knowledge of commonly-used concepts, practices, and procedures within the field.

Incumbent is held accountable for following appropriate policies and procedures regarding protecting the availability and security of the organizational footprint.

Incumbents must be able to work with limited supervision and exercise independent judgment.

Maintain documentation of problems reported and resolutions.

Actively participate in organizational monitoring for suspicious activity.

Technical knowledge necessary to manipulate/modify risk-mitigating devices (firewalls, network access control, IPS/IDS, Privilege Identity Management, malware mitigation, web proxy, etc.).

Provide technical support to the Help Desk in resolving end-user access or application issues.

Ability to comply with Help Desk service standards and provide good customer service is required.

Actively participate in the sales and service culture, support the values of the organization, and follow established holding company policies and procedures

## Requirements

Bachelor’s degree in Information Technology specializing in IT Security along with two years of practical experience. Prior employment experience within the technology and security-related fields may be substituted for educational requirements.
Security certifications are highly desirable.
Must be able to handle stress and establish priorities.
Must be courteous, able to handle frequent deadlines, and interact with people.
Duties and responsibilities require judgment, initiative, and attention to detail.
Candidate must possess the ability to function well in a rapidly changing environment with little direct supervision.
Professional demeanor is essential.

# Security Administrator  3

## Job summary

We are looking for a Security Administrator. The Alternate Contractor Program Security Officer (ACPSO) provides oversight of Program security within a multi-disciplinary environment including collateral and SAP/SAR materials.

## Responsibilities

Maintain security team coverage on-site during core business hours from 0800 until 1600 Monday through Friday, and act as an on-call backup in responding to alarms after core business hours as required.
Communicate with multiple Government Agencies and assist as a liaison between Program Manager, Program Security Manager, Facility Security Officer, and other Government personnel and industry partners for access requests, visit certifications, and document control-related tasking.
Ensure compliance with policies and procedures by the DoD Manual 5205.07 Vol(s) 1-4, ICD 705 series, SECNAV M-5510.30, Intelligence Community Directive 705 series, National Industrial Security Program Operating Manual (NISPOM).
Preparation, implementation, tracking, and maintenance of security plans, Standard Operating Procedures (SOPs), and other relevant Program materials and documentation.
Responsible for initial personnel access requests, facilitating updating personnel periodic and annual reporting requirements, briefing and debriefing personnel on appropriate policies, security guidelines, and other security admin and document control requirements.

Assisting with annual self-inspections, security compliance inspections, facilitating the transmission of materials, tracking facility inventory, and other facility communication & equipment capabilities.

Assisting in escorting visitors & maintenance personnel.

## Requirements

Bachelor's Degree and 2 years experience. Additional years of experience may be substituted instead of a degree.

Experience with DoD 5205.07 Vol(s) 1-4, Intelligence Community Directive 705 series, SECNAV M-5510.30, NISPOM; as well as other applicable DoD, IC, and National level security directives.

Experience in physical security.

Experience in document control & inventory management.

Excellent verbal and written communication skills are essential.

# Security Administrator  4

## Job summary

The <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> within the IT Central Security Administration group will perform daily IT Security administration for all major client-accessible platforms and supported application software. This position is responsible for the daily provisioning/de-provisioning of security to IT Systems

## Responsibilities

Ensuring adherence to Cyber Security Policy, FERC, CIP, SOx, security standards/procedures/guidelines in all daily activities; following Central Security Admin procedures for all requests

Independently process client requests for Active Directory-based application access, SAP position-based security administration requests, and RAAD requests for CIP/BCSI access

Assess security requirements and process adjustments for transfers and separations

Performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction.

Interface with Compliance, Cyber Security, Security Operations, and Application Support Teams to identify security access configuration requirements and procedures for appropriately granting/removing security access.

Interact with the user community to understand their security needs and process requests appropriately.

Participate in the On-Call rotation 24x7, once every 6 weeks, after being onboarded to the team and comfortable

## Requirements

Associates Degree or greater in a related field. Instead of a degree, 2+ years of related experience.

Related experience includes, but is not limited to: experience in an IT-related field, identity management, desktop support, and service desk.

Demonstrate strong organizational skills and attention to details

Ability to read and accurately follow procedures promptly.

Strong communication skills (written and verbal).

Excellent customer service skills, including the ability to be friendly, courteous, and helpful toward internal customers

Strong analytical and problem-solving skills.

Ability to work in a fast-paced environment.

Demonstrate a questioning attitude to continue to learn.

Ability to work independently with an understanding of core teamwork skills.

# Security Administrator  5

## Job summary

The <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> in support of Field Office operations throughout the Bureau of Diplomatic Security. The selected individuals will perform a variety of operational, administrative, and coordination duties, will provide general administrative support, and maintain various administrative reports.

## Responsibilities

Provide data entry, extraction, analysis, and reporting for various databases currently in use, under development, or planned for the various functions of the program office, including assisting in establishing production databases for operational systems, as required;

Provide document processing and writing support for the administrative and program activities;

Maintain files of sensitive and classified documents and post changes to required materials;

Assist in the preparation, coordination, delivery, and follow-up actions on assigned program operations;

Create and maintain flow charts, spreadsheets, and documents as assigned;

Maintain file organization;

Provide administrative support for status reports, briefing presentations, and special projects;

Prepare charts, tables, graphs, and diagrams to assist in tracking and reporting program activities;

Assist in the preparation of all reports and tracking documents including budgets, monthly reports, personnel tracking, etc.;

Peorm other duties as assigned.

## Requirements

Undergraduate degree and 2 years specialized office experience preferred OR High School diploma or GED equivalent and 5 years of specialized administrative experience;
Specialized experience includes office management, expense tracking, review of executive level correspondence, database administration, financial and project status tracking and reporting, monthly reports, and maintaining operating procedures;
Extensive knowledge of electronic database operations management, administrative and correspondence processing procedures, and understanding of procedures required for processing actions for review, approval, and release;
Must possess strong editorial, clerical and analytical skills and the willingness to learn any specific program requirements of the position;
Must be proficient with Microsoft Word; have basic skills with Excel and PowerPoint; and other database software experience desired.
Must have excellent organizational skills and the ability to work in a fast-paced environment to meet deadlines and handle high-pressure situations.

# Security Administrator  6

## Job summary

We have an opportunity for a <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> to support our government customer. In this role, you will work closely with our Contractor Program Security Officer (CPSO) in executing day-to-day security program requirements. This is an excellent opportunity to grow your career in the program security field!

## Responsibilities

Assisting in the creation and routing of documentation/reports detailing security incidents that occur within the office.
Maintaining applicable program directives, regulations, manuals, and guidelines.
Properly accounting for, controlling, transmitting, transporting, and safeguarding sensitive material and documents.
Assisting in certifying and receiving visitor clearances and accesses.
Maintaining DISS to reflect personnel under sites' cognizance.
Assisting management in the oversight of program personnel, information, and physical and technical security actions and procedures.
Providing technical assistance with the processing of eligibility requests.

## Requirements

High school diploma or equivalent is required.
Two (2) years of experience assisting a Program Security Official (or related) is desired.

Two (2) years of experience generating and tracking visit certification entering and leaving the facility, desired.

Ability to develop and maintain positive working relationships with internal and external customers.

Proficiency with MS Office (Outlook, Word, Excel, and PowerPoint)

Some experience with/knowledge of DISS, EPSQ/e-QIP is desired.

Effective written and verbal communication skills.

Proactive attitude with the ability to work with minimal supervision.

Demonstrated critical thinking and problem-solving skills.

Able to prioritize competing tasks and remain organized.

# Security Administrator  7

## Job summary

This position will work as a <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> for the security program reporting to the Director, Corporate Security. The person will perform security services as the main classification document reviewer to ensure proper handling, marking, downgrading, and declassification recommendations are in full compliance with the National Industrial Security Implementation Manual (NISPOM), policy directives, and other security classification guides as mandated. Interprets and ensures compliance with established guidelines, procedures, and policies.

## Responsibilities

Review material from both internal and external sources to determine security classification and handling requirements by the Department of Defense (DoD), Navy, Marine Corps, and other government agencies.

Assist in conducting internal investigations on matters concerning security violations, misconduct, and other charges involving security classification mishaps. Consult with and support the Compliance Committee on internal investigations, as required.

Stay up-to-date on current security industry issues, and maintain positive relationships within the security community.

Assist the Director, of Corporate Security as needed on special projects.

Perform other duties as assigned.

## Requirements

Education: Bachelor’s degree in a related field or equivalent combination of education and qualified security work experience.

Experience: Minimum of 6 years related experience as a document reviewer, including extensive administrative background and work in a DOD environment.

Skills: Must have proven customer service skills; computer literacy and proficiency; excellent oral and written communication skills, working knowledge of NISPOM, JAFAN, and familiarity with ICD and DCIDs.

# Security Administrator  8

## Job summary

The Security Administrator's role is to function as a <a href="https://100hires.com/subject-matter-expert-job-description.html">Subject Matter Expert</a> (SME) over security standards and configurations for Windows, Active Directory, and Azure (Cloud). This includes consultation and technical support for projects and ITSM tickets. The <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> will oversee the proper creation and implementation of security standards for all IT assets in their assigned scope. As part of their SME function, they will work with project teams, other technology groups, and other lines of business to consult on projects. The <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> is expected to learn, understand, and ensure compliance with all regional and global IT policies.

## Responsibilities

Provides support, implementation, and design services for Microsoft Active Directory and Windows-based systems (Client, Server, AD, Azure) across the enterprise.

Applies new solutions through research and collaboration with the team and determines the course of action for new application initiatives.

Implements new software solutions as required by the business with Global, Regional, or Local impact.

Resolves and appropriately completes assigned cases/incidents and change requests and acts as an escalation for support issues.

## Requirements

Bachelor’s degree in Information Systems, Computer Science, Engineering, or a related technical discipline, or the equivalent combination of education, technical training, or work/military experience.

Knowledgeable in Security and Control Frameworks, such as ISO 27002, NIST, COBIT, COSO, and ITIL;

5+ years as an Information Security and/or Windows Systems Administrator

3+ years of directly related experience supporting Active Directory operations and engineering with increasing responsibility.

5+ years of combined IT and security work experience with a broad range of exposure to systems analysis, applications development, database design, and administration.

2+ years experience with Microsoft Azure

Must possess proven experience working with a large enterprise distributed computing environment. These experiences should include:

Directory Services Infrastructure architect/design/support in a Multi-domain forest

Strong understanding of architecting and configuring Microsoft Windows OS technology including AD Forests, Domains, Trusts, DNS, DHCP, Group Policy, and Organizational Units.

Azure AD identity Management, Configure Azure AD SSO using SAMLOAUTHOIDC Protocol

Manage Azure AD permissions and Trust relationships, Manage Forest/Domain/OU/User Object management

Application of industry security standards to enterprise configurations, settings, and security controls

# Security Administrator  9

## Job summary

We're seeking an experienced <a href="https://100hires.com/security-administrator-job-description.html">Security Administrator</a> to join our Information Technology team. Supports project teams using a wide range of developing professional skills while working independently with guidance. Focuses on configuring systems related to external/customer Identity and Access Management (IAM) systems. Collaborates on a broad range of tasks including administration of information security tools and devices, security information, and event management. Strong written and interpersonal communication with all levels in the organization.

## Responsibilities

Performs remedial actions because of threat and vulnerability assessments or audits

Monitors and analyzes unusual or suspicious activity and makes recommendations for resolution

Interacts closely with product vendors and service providers, with personnel from various IT departments including the application development, operations, and network teams

Trains others on the use of security tools and resolution of security issues

Researches, recommends, evaluates, and implements information security solutions

Recommends, schedules, and applies patches, removes or otherwise mitigates known control weaknesses

## Requirements

Professional degree in Computer Science or an equivalent combination of education and experience

Typically with 2+ years of experience in cyber security incident response & remediation activities

Information Security Certification (CISSP, CISM) preferred

Experience with security solutions such as Okta, Crowdstrike, SumoLogic, Microsoft Cloud App Security, Carbon Black, and Cisco Umbrella preferred

Experience in MS Office Suite, including Excel, Outlook, and Word

Strong customer service, interpersonal skills, and the ability to interact with all levels of staff

Strong work ethic and eagerness to produce high-quality, accurate results

Ability to hold sensitive information with a high level of confidentiality and integrity

Ability to communicate and present ideas in a clear, concise, and professional manner both verbally and in writing

Ability to proactively problem solve and apply innovative solutions

Ability to work and collaborate in a team environment, and ability to work independently and prioritize work

Ability to work on multiple projects at the same time

Ability to effectively meet deadlines at expected quality

# Security Administrator  10

## Job summary

We are looking for a Security Administrator.

## Responsibilities

Work collaboratively with a team to design, configure and deploy security frameworks, devices, and applications

Respect confidentiality of all requests

Enforce JBS security configurations and standards in all projects or implementations

Enforce security compliance and best practices on all projects or implementations

Use tracking systems to keep an exact record of each request/configuration/design and the action taken

Escalate to IT manager whenever conflicts in access is discovered

Troubleshoot complex security issues

Audit and assist in the execution of ethical hacking of our network frameworks and applications

Complete projects in a timely manner

Advise customers on access and data security practices

Communicate in a polite, confident, professional, and easy-to-understand the manner

Communicate with 3rdparty application providers, when necessary, on security initiatives

Configuration, deployment, and maintenance of security tools and applications

Other duties as assigned

## Requirements

Requires a Bachelor’s Degree in Information Systems or a related field

4+ years in the IT industry

Familiarity with critical business systems

2+ years direct IT Security experience

Experience with Active Directory, Windows Security/Administration, DNS management, network security, and SEIM tools

Solid understanding of infrastructure technologies

Excellent communication skills

Excellent attention to details

Outstanding organizational and analytical skills

Excellent customer service skills

Able to work independently and inside a team

As a salaried position with the company, you may be required to travel at some point to other facilities, to attend Company events, or as a representative of the Company in other situations. Unless otherwise specified in this posting, the amount of travel may vary and the most qualified candidate must be willing and able to travel as business needs dictate.