



Information Technology Job Family: **IT Security Engineer Progression**

These generic job title summaries are intended to indicate the kinds of tasks and levels of work complexity that will be required of positions classified to any of these titles and are not intended to be construed as declaring the specific duties and responsibilities of any particular position. The use of particular expressions or illustrations describing functions within a specific job title does not exclude other duties of a similar kind and/or level of complexity. Positions are classified to a particular job title based upon the predominant level of expected work complexity. ***A position that is classified into this title and band must meet the Cornell requirements for exemption under the FLSA***

GENERIC JOB PROFILE SUMMARIES

IT Security Engineer III INDIVIDUAL CONTRIBUTOR	IT Security Engineer IV INDIVIDUAL CONTRIBUTOR	IT Security Engineer V INDIVIDUAL CONTRIBUTOR
	Serve as technical lead for larger projects and manage focused technical projects; collaborate with service owners to define scope of work required to interface their applications with central identity systems.	Lead large projects and direct and manage focused technical projects; oversee the collaboration with service owners to define scope of work required to interface their applications with central identity systems.
Develop, implement and promulgate standard approaches and solutions for securing systems.	Define, review and enforce information security policy, standards and guidelines for business operations and technology implementations.	Lead, support and manage the development, implementation and promulgation of standard approaches, solutions and best practices for securing the campus IT infrastructure; develop and implement appropriate security controls to maintain compliance with security and/or privacy legislation.
Evaluate and respond to reports of computer compromise or abuse; investigate, analyze and counter system intrusions and compromises; perform regular monitoring and analysis of systems and networks, reporting on trends and anomalies.	Proactively identify IT security risks including IT technical implementations or business processes; evaluate and develop approach to solutions.	
Conduct security assessments and audits, penetration testing, and incident management.	Define, review, implement and promulgate approaches, services and tools for security assessment and audits, penetration testing and incident management	
Participate in security project implementations.	Assume responsibility for the planning and implementation of major upgrades to the existing infrastructure on a regular timetable.	Assess existing and new technologies; propose new or significantly enhanced systems, applications and processes.

IT Security Engineer III INDIVIDUAL CONTRIBUTOR	IT Security Engineer IV INDIVIDUAL CONTRIBUTOR	IT Security Engineer V INDIVIDUAL CONTRIBUTOR
Partner with software development teams to define security objectives and guidelines.		
Coordinate department-wide IT Security matters such as incident response, intrusion detection management and IT Security advisories.	Provide a complete range of incident response services including threat assessment, preventive and corrective action, system remediation, investigation and analysis; collaborate in the on-going refinement of incident response processes, including development of detailed operational procedures.	Lead and direct a complete range of incident response services including threat assessment, preventive and corrective action, system remediation, investigation and analysis; lead the collaboration in the on-going refinement of incident response processes.
Proactively assesses potential items of risk and opportunities of vulnerability in the network.	Proactively assesses potential items of risk and opportunities of vulnerability in the network; determine when permanent or temporary changes to network infrastructure necessary to maintain campus security, including blocking specific internal or external hosts and sites.	Develop and provide risk assessment mechanisms to support university regulatory and IT compliance requirements.
		Lead the Security Engineering team in the design, implementation and maintenance of new and updated security services such as network scanning, security audits, security architecture consulting.
	Develop, design, and implement a Security Incident Response Program; develop program specifications, including both server hardware and software evaluation.	
Work closely with appropriate vendors to resolve issues and evaluate new products.	Negotiate with vendors for software licenses for campus availability, including configurations, numbers of individual licenses, pricing and availability dates (pre-releases); work closely with appropriate vendors to resolve issues and evaluate new products.	
Operate a campus-wide service such as vulnerability scanning, encryption and security management console.	Develop and maintain a campus-wide service such as vulnerability scanning, encryption and security management console.	
Design program specifications to include campus-wide server criteria as well as specific infrastructure related criteria.	Develop complex program specifications to include campus-wide server criteria as well as specific infrastructure related criteria.	Develop and design highly complex program specifications to include campus-wide server criteria as well as specific infrastructure related criteria.
	Consult with and advise senior engineering members of the staff in areas concerning system and network security configurations.	Advise senior engineering members of the staff in areas concerning system and network security configurations.

IT Security Engineer III INDIVIDUAL CONTRIBUTOR	IT Security Engineer IV INDIVIDUAL CONTRIBUTOR	IT Security Engineer V INDIVIDUAL CONTRIBUTOR
Research, recommend, design, develop, evaluate, enhance test plans and implement tools as needed in support of security issues and client/server based security tools.	Research, recommend, design, develop, evaluate, enhance complex test plans and implement tools as needed in support of security issues and client/server based security tools.	
	Participate in and contribute to relevant discussion groups and national technical forums to validate Cornell's technical direction with representatives from peer institutions.	Participate in and contribute to relevant discussion groups and national technical forums to validate Cornell's technical direction with representatives from peer institutions.
Install, operate and maintain a diverse array of technologies related to systems and network security including SEIM, IDS/IPS, network vulnerability scanners, firewalls, access control and authentication mechanisms, anti-virus software, plus ad hoc tools for analysis, reporting, task automation.	Research, evaluate, test, recommend, implement and maintain a diverse array of technologies related to systems and network security including SEIM, IDS/IPS, network vulnerability scanners, firewalls, access control and authentication mechanisms, anti-virus software, plus ad hoc tools for analysis, reporting, task automation.	Lead and manage the research, evaluation, testing, recommendations, selection, implementation, development and maintenance of a diverse array of technologies related to systems and network security including intrusion detection systems, network scanners, firewalls, honeypots, network access control mechanisms, anti-virus software, plus ad hoc tools for analysis, reporting, task automation.
	Develop tools, software, and Web services to deliver security technologies; collaborate in the design and realization of the overall security infrastructure.	Lead the design and realization of Cornell's overall security infrastructure.

JOB FACTOR PROFILE TABLE

FACTOR PROFILE	11492 IT SECURITY ENGINEER III, BAND F	11493 IT SECURITY ENGINEER IV, BAND G	11494 IT SECURITY ENGINEER V, BAND H
MINIMUM EDUCATION AND EXPERIENCE EQUIVALENCY	Bachelor's degree; more than 3 years and less than 5 years experience or equivalent.	Bachelor's degree; more than 5 year and less than 7 years experience or equivalent.	Bachelor's degree; more than 7 years and less than 10 years experience or equivalent.
IMPACT	Moderate impact	Moderate impact	Substantial impact
CONTACTS - INSIDE	Provide guidance to others Coordinate activities	Provide guidance to others Coordinate activities	High-level interaction Involved in diverse and highly sensitive or confidential activities
CONTACTS - OUTSIDE	Provide information that exists within pre-established documents or programs	Provide/receive guidance, advice or information that must be analyzed and developed by the position	Provide/receive guidance, advice or information that must be analyzed and developed by the position
CONTACTS - STUDENTS	Frequent contact to provide information and instruction	Frequent contact to provide information and instruction	Limited contact

FACTOR PROFILE	11492 IT SECURITY ENGINEER III, BAND F	11493 IT SECURITY ENGINEER IV, BAND G	11494 IT SECURITY ENGINEER V, BAND H
SUPERVISION	Day-to-day supervision to employees within the dept	Provide supervisory direction to other supervisors	Provide supervisory direction to other supervisors
COMPLEXITY	Frequently adapt, combine, or make improvements to services, products, processes, & programs. Work requires reasoning skills and judgment	Occasionally required to develop new innovative solutions, services, products, processes, & programs. Work requires sophisticated reasoning skills	Continually required to develop new innovative solutions, services, products, processes, & programs. Work requires conceptual and imaginative thinking in a highly complex environment
LEVEL OF DECISION MAKING	Responsible for assisting in and influencing decisions concerning policy-setting, research, planning, or students	Responsible for making decisions regarding policy-setting, research, planning, or students	Responsible for making decisions regarding policy-setting, research, planning, or students
FREEDOM OF ACTION	Very general supervision Interpretation of work policies and procedures, and, at times deviation from standard work practice	Very general supervision Interpretation of work policies and procedures, and, at times deviation from standard work practice	Little direct supervision Considerable latitude for exercising judgment and self-direction
EFFECT OF DECISION MAKING	Directly effects entire department Moderate effect on students and employees	Directly effects entire department Moderate effect on students and employees	Directly affect entire college or school administrative unit Critical effect on students and employees
WORKING CONDITIONS	Normal working conditions, including limited or no exposure to hazardous conditions/materials/ equipment. Safety gear may sometimes be required	Normal working conditions, including limited or no exposure to hazardous conditions/materials/ equipment. Safety gear may sometimes be required	Normal working conditions, including limited or no exposure to hazardous conditions/materials/ equipment. Safety gear may sometimes be required