Security Policy and Procedure Development Training Course



26 - 30 Oct 2026

Boston

7500 € (Per Person)

Ref: #SM9944_131476

Course Introduction / Overview:

In today's complex operational landscape, a robust security posture is not a luxury but a necessity for organizational survival and success. The foundation of any effective security program lies in well-crafted, comprehensive security policies and clear, actionable Standard Operating Procedures (SOPs). This course provides a deep dive into the art and science of creating these critical documents. Moving beyond generic templates, this program, offered by BIG BEN Training Center, equips participants with the skills to develop, implement, and manage security frameworks that are aligned with business objectives, compliant with regulatory standards, and resilient against emerging threats. Drawing on principles outlined by security management experts like Charles A. Sennewald in his seminal work "Effective Security Management," the curriculum emphasizes a proactive, risk-based approach. Participants will learn to translate high-level security governance into practical, on-the-ground procedures that protect assets, ensure operational continuity, and foster a culture of security awareness throughout the entire organization, from the server room to the front desk. This is a masterclass in building the documented backbone of a truly secure enterprise.

Target Audience / This training course is suitable for:

- Security Managers and Directors.
- IT Security Professionals and System Administrators.
- Compliance Officers and Auditors.
- Operations Managers and Team Leaders.
- Facility and Physical Security Managers.
- Human Resources Professionals.
- Risk Management Specialists.
- Project Managers responsible for security-related initiatives.
- Anyone tasked with writing or overseeing corporate policies and procedures.

Target Sectors and Industries:

- Banking, Finance, and Insurance Services.
- Healthcare and Pharmaceutical Industries.
- Information Technology and Telecommunications.
- Government Agencies and Public Sector Bodies.
- Manufacturing and Industrial Operations.
- Retail and E-commerce.
- Energy and Utilities.
- Education and Research Institutions.
- Transportation and Logistics.

Target Organizations Departments:

- Corporate Security Department.
- Information Technology (IT) and Cybersecurity.
- Legal, Risk, and Compliance.
- Human Resources (HR).
- Operations and Production.
- Facilities Management.
- Internal Audit.
- Executive Management.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a comprehensive security policy framework from the ground up.
- Write clear, concise, and legally sound Standard Operating Procedures (SOPs).
- Align security policies with international standards like ISO 27001 and NIST frameworks.
- Conduct thorough risk assessments to identify vulnerabilities and inform policy content.
- Master the policy lifecycle, including drafting, review, approval, and retirement.
- Design effective communication and training plans for policy implementation.
- Establish metrics to monitor policy compliance and effectiveness.
- Create robust incident response and business continuity procedures.
- Integrate physical, personnel, and information security policies into a cohesive strategy.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, practical, and engaging, ensuring that participants leave with tangible skills they can apply immediately. We believe that adult learning is most effective when it moves beyond passive listening to active participation. The course is structured around a blend of expert-led instruction, real-world case study analysis, and collaborative group workshops. Participants will engage in hands-on exercises, such as drafting sample policies for fictional scenarios, critiquing existing SOPs for clarity and effectiveness, and developing a policy implementation roadmap. Interactive sessions, facilitated discussions, and peer-to-peer feedback are central to the learning process, allowing for the exchange of diverse perspectives and experiences. Our approach emphasizes problem-solving and critical thinking, challenging participants to tackle complex security governance issues. This immersive learning environment ensures a deep understanding of the principles and practices of security policy and procedure development, transforming theoretical knowledge into practical mastery.

Course Agenda (Course Units):

Unit One: Foundations of Security Policy and Governance

- The Role of Policies and Procedures in Risk Management.
- Distinguishing Between Policies, Standards, Procedures, and Guidelines.
- Understanding the Security Governance Framework.
- Key Legal, Regulatory, and Compliance Drivers (e.g., GDPR, HIPAA).
- Aligning Security Strategy with Business Objectives.
- The Psychology of Policy Adherence and Corporate Culture.
- Stakeholder Analysis and Management in Policy Development.

Unit Two: The Policy Development Lifecycle

- Phase 1: Needs Analysis and Scoping the Policy.
- Phase 2: Information Gathering and Risk Assessment Methodologies.
- Phase 3: Drafting the Policy - Structure, Tone, and Language.
- Phase 4: The Review and Consultation Process.
- Phase 5: Gaining Senior Management Approval and Ratification.
- Phase 6: Version Control and Document Management Best Practices.
- Introduction to Policy Management Software and Tools.

Unit Three: Crafting Effective Standard Operating Procedures (SOPs)

- The Purpose and Benefits of Clear SOPs.
- Choosing the Right SOP Format (Checklist, Hierarchical, Flowchart).
- Writing for the User: Clarity, Brevity, and Action-Oriented Language.
- Developing SOPs for Technical and Non-Technical Audiences.
- Integrating Visual Aids and Diagrams into Procedures.
- Testing and Validating SOPs Before Deployment.
- Managing SOP Revisions and Updates Systematically.

Unit Four: Core Security Policy Domains

- Information Security and Data Classification Policies.
- Access Control Policies (Physical and Logical).
- Acceptable Use Policy for IT Resources.
- Physical Security and Asset Protection Policies.
- Incident Response and Reporting Procedures.
- Business Continuity and Disaster Recovery Planning.
- Workplace Violence Prevention and Personnel Security Policies.
- Third-Party and Vendor Security Management Policies.

Unit Five: Implementation, Communication, and Continuous Improvement

- Developing a Strategic Policy Roll-Out Plan.
- Creating Effective Security Awareness and Training Programs.
- Communicating Policies to a Diverse Workforce.
- Monitoring Compliance and Handling Non-Compliance.
- Conducting Policy Audits and Effectiveness Reviews.
- Establishing Key Performance Indicators (KPIs) for the Security Program.
- The Process for Policy Maintenance, Updates, and Retirement.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In an era of constantly evolving cyber and physical threats, how can an organization create security policies that are both robust enough to be effective and flexible enough to adapt without stifling innovation?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic and integrated approach to security documentation. Unlike programs that focus narrowly on either IT security or physical security, this curriculum teaches participants how to weave these disparate domains into a single, cohesive governance framework. The emphasis is not merely on what a policy should contain, but on the entire lifecycle—from the initial risk assessment that justifies its existence to the communication strategies that ensure its adoption and the audit processes that verify its effectiveness. A significant differentiator is our focus on the "human factor," exploring the psychology behind policy compliance and providing strategies for writing documents that are not just technically sound but also clear, practical, and user-centric. While other courses may provide templates, this program equips participants with the critical thinking and analytical skills to develop bespoke policies and procedures that are perfectly tailored to their organization's specific culture, risk appetite, and operational realities. The hands-on workshops and case-study-driven methodology ensure that participants leave with the confidence to build a security framework that is both compliant and truly effective.