ASCENT
Security Compliance Portal

TOP STEPS FOR IMPLEMENTING A PERSONNEL SECURITY PROGRAM

Here's how to implement and maintain a strong personnel strategy and program to protect your business.

Why does it seem that some of the most important things in life are often those that are the most overlooked? For example, a Personnel Security Program is a vital part of any organization, but personnel security is often the part of the overall corporate Security Program that is lacking the most.

An effective Personnel Security Program is necessary to protect your people, information, and assets by enabling your organization to reduce the risk of harm to your people, customers, and partners, as well as reduce the risk of your information or assets being lost, damaged, or compromised. The objective of an effective Personnel Security Program is to help an organization make a reasonable determination that individuals granted access to classified information or assigned to sensitive positions are and will remain loyal, trustworthy, and reliable.

To help you implement and maintain a strong personnel strategy and program for your organization, consider the following tips. They will help you have greater trust in people who access your official or important information and assets and deliver services and operate more effectively.

1. Define roles and responsibilities. Security roles and responsibilities for all appropriate personnel should be defined and documented. Every position throughout the organization that plays a role in managing or complying with security controls should have their applicable roles and responsibilities documented. Your CISO, or similarly titled role, should partner with the HR team to ensure roles and responsibilities are appropriately outlined and to maintain a plan for talent recruitment and retention. Succession planning is also important to ensure the Security Program continues to succeed as personnel are promoted, transferred, or depart the organization.

2. Perform pre-employment screening for personnel. All personnel need to be screened prior to starting employment to ensure organizations hire knowledgeable, ethical individuals with the appropriate skill sets and experience to fill open positions. Whatever screening process is deemed appropriate for an organization, procedures should be documented to ensure organizations follow standard processes to successfully complete personnel screening in a repeatable and reliable manner.

An effective Personnel Security Program will help you have greater trust in people who access your official or important information and assets.

3. Document terms and conditions of employment. As part of their contractual obligations to an organization, personnel should agree to, and sign the terms and conditions of their employment. This ensures organizations are protected and supports the organizations' abilities to hold personnel accountable if any issues arise during employment. Terms and conditions should state that all personnel provided access to protected or sensitive information are required to sign a confidentiality or non-disclosure agreement prior to being provided access.

4. Define and communicate management responsibilities. Managers of all departments should be responsible and accountable for ensuring their teams perform the assigned functions within their areas of responsibility in accordance with defined Security Program controls. Security risks and control requirements should be actively discussed at business unit meetings. Managers often lead by example, so if a manager "colors outside the lines," it is a safe bet that their teams will eventually do the same. Managers should ensure their teams have a clear understanding of how to identify and escalate potential security issues to appropriate security personnel.

5. Spearhead a Security Awareness Training Program. Organizations should develop, document, and maintain a comprehensive Security Awareness Training Program. This needs to include security control updates made to the organization's security policies, plans, and procedures that are relevant to their job function. Training should also include information on security best practices. At a minimum, security awareness training should be completed as part of initial training for newly hired personnel and annually thereafter for all personnel. Training should also be provided whenever required by the system, security control, or operational changes.

6. Ensure a disciplinary process is in place. Organizations should implement, communicate, maintain, and provide training on a formal disciplinary process for personnel that violates controls contained in

security policies or commits a security incident. While punitive actions are not ideal, if "bad" behavior is not corrected, it is likely to continue, putting organizations at risk unnecessarily. All appropriate personnel should be aware of the potential discipline associated with not following prescribed controls. Organizations need to ensure the same types of situations are handled in a comparable manner to preclude unfair treatment of personnel.

7. Plan for termination of employment or position changes. A process needs to be defined by organizations to address the security control requirements associated with the termination of personnel or changes in the position of personnel from one role to another. This is required to ensure access is terminated in a timely fashion, or appropriately adjusted when personnel transfer from one role to another. A documented termination checklist helps to ensure all planned steps are taken upon the termination of personnel. Organizations put the confidentiality of information at risk if appropriate access revocation or modification is not completed in a timely manner.

Your organization should ensure that a comprehensive Personnel Security Program is developed and implemented consistently across the organization. Organizations that do not could potentially overlook a pivotal security function or leave a control unaddressed.

Organizations without a comprehensive Personnel Security Program can potentially overlook a pivotal security function or leave a control unaddressed.

By developing a personnel security strategy and building a comprehensive Personnel Security Program, supported by all organizational stakeholders, organizations can avoid key personnel security pitfalls for effective overall security.

READ MORE > 100 Security Program Pitfalls and Prescriptions to Avoid Them.

ASCENT Portal - A Single Source of Security and Compliance Truth

Automate, Manage and Track All Your Compliance Processes Across More than 40 Industry Frameworks

The ASCENT Portal is a comprehensive SaaS-based platform that delivers fingertip access to everything you need to comply with more than 40 industry frameworks. From customizable assessments and calendar-driven control task reminders to governance templates and compliant vendor management, the ASCENT Portal automates your compliance process, end-to-end, while delivering real-time status views and reports all from a single source.

Schedule a demo today.

SCHEDULE A DEMO

ASCENT
Security Compliance Portal

ASCENT Portal
Capital View Center , 1301 S. Capital of Texas Highway, Suite A-130, Austin, TX 78746

Phone: 866.300.0795 **Email:** sales@ascent-portal.com **Web**: www.ascent-portal.com