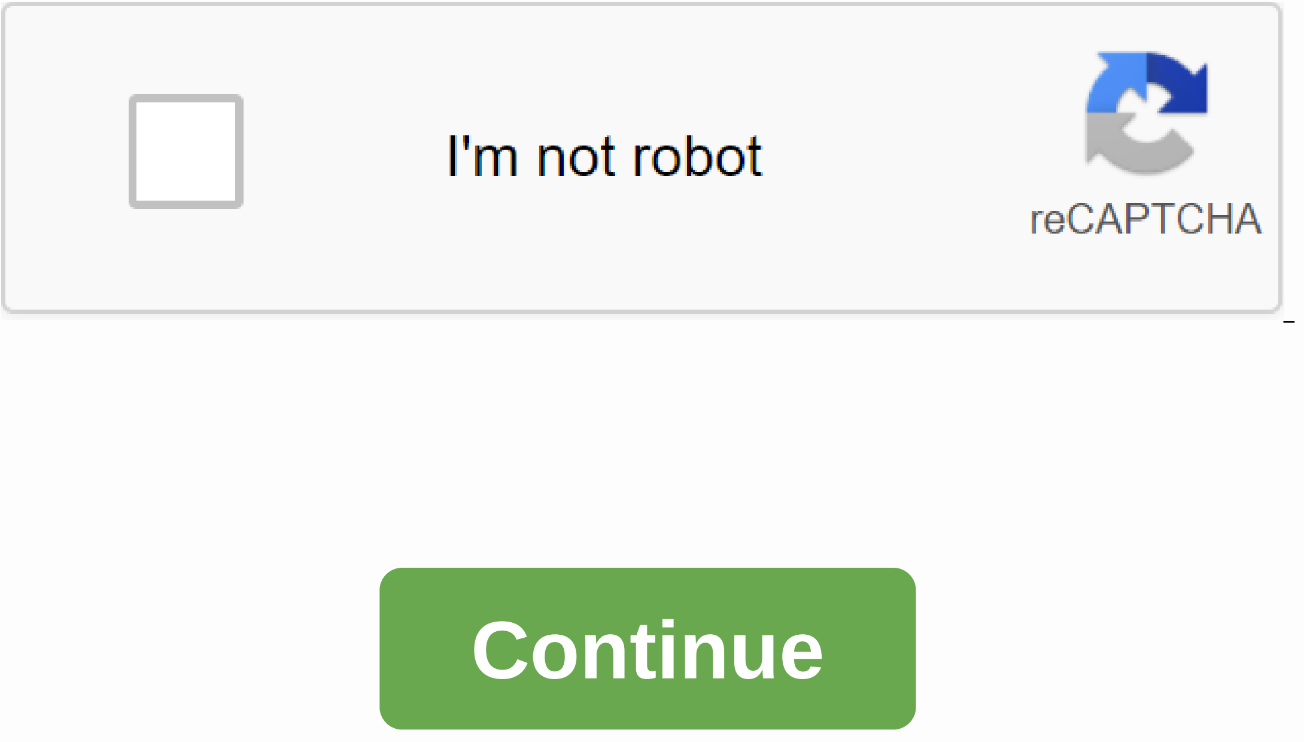

□ I'm not robot

reCAPTCHA

Continue

The handbook of fixed income securities pdf

Supplemental Security Income (SSI) Supplemental Security Income is a federal program funded by general funds of the United States Treasury. The U.S. Social Security Administration (SSA) manages the program, maSSI is not paid by Social Security taxes. SSI provides financial support to disabled adults and children with limited income and wealth. Returning to benefit categories, I wrote two days ago about a report recommending eliminating the option to collect Social Security at the age of 62. The author, who is affiliated with the conservative think tank American Enterprise Institute, also advocated abandoning Social Security disability as it is and eliminating Social Security taxes for workers who have worked more than 35 years. I got a couple of responses from readers who thought this pension planning proposal was bad, including a strong raspberry from my Bankrate colleague Barbara Whelehan, who shares this retirement blog with me. Barbara said: You make a good case, but I have to say I agree with Mary (another reader who commented) - raise the cap on Social Security taxes so that high incomes don't get a break. Why should low- and middle-income workers pay all their income, but high-income workers only pay taxes up to $106,800 of their earnings? Lifting the roof would help make Social Security solvent for another 75 years, a topic I made in a recent blog here about Bankrate. ... The American Academy of Actuaries calculates that gradually raising the annual earnings cap from $106,800 to cover 90 percent of all wages (the current cap covers about 83 percent of all wages) and using the higher ceiling to calculate benefits, too, would solve 37 percent of the social security shortage -- but of course not everything. To solve all this, you should eliminate the cap and ask high-income workers to pay Social Security tax on all their earnings, but only calculate earnings benefits up to the current ceiling. Barbara says: I'm voting to raise the income ceiling, but not the payments. With all due respect, Barbara, I think it's totally unfair. Raising Social Security taxes without increasing the amount that people who pay those taxes get in benefits would be a huge tax increase for people who aren't actually that rich. Earning $106,800 is a good income, but bill gates doesn't make you, especially in the high-cost parts of the country. Actuaries outline various alternative scenarios, but none of them are perfect, and all those that eliminate the entire deficit result in performance cuts or taxes. Nothing surprising there, but no matter how you cut it, it's painful for someone, and I think the level of pain on your proposal is uncceptably high. Will your retirement plan allow you haute cuisine in exotic places? Or makeshift dinners with your neighbors? Request a free makeover of money to be present in Bankrate Bankrate's next retirement Series. September 17, 2016 2:20 AM ET Order Risprints Print Article The Bipartisan Policy Center is trying to make the most of its name, an easy task in the bloc's national capital. The centre has published a report by its Pension Security and Personal Savings Commission entitled Securing Our Financial Future. It also needs a subtitle: How to Touch the Third Rail of American Politics and Live to Tell About It could be a good one. Social security reform is one of its important issues. But it's politically and financially realistic. After 2 and a half years of bargaining, the members divided the... The Bipartisan Policy Center is trying to be at the foot of its name, a not easy task in the nation's stalled capital. An error occurred, please try again later. Thank you This article was submitted as of May 4, 2020 Purpose (1) This broadcasts revised IRM 1.4.6, Resource Guide for Managers, Managers Security Handbook. Material Changes (1) This IRM has been updated to reflect the titles, scope, definitions, and authorized use of the current organization. (2) IRM 1.4.6.2, Responsibility for Facilities Management and Security Services has moved to IRM 1.4.6.1, Scope and Objectives. (3) IRM 1.4.6.3, Management Responsibility has moved to IRM 1.4.6.1, Scope and Objectives. (4) Removed IRM 1.4.6.7.8, Calling Cards. Business cards are no longer considered an authorized form of IDENTITY support, for IRM 10.2.18, Physical Access Control (PAC). (5) Removed IRM 1.4.6.7.3, Issuance of identity cards to non-federal personnel. (6) Removed IRM 1.4.6.7.4, Issuing identity cards for visitors. (7) Removed IRM 1.4.6.7.5, Escort Only ID cards. (8) Removed Annex 1.4.6-1, Alternate Security Chart. Refer to IRM 10.2.15, Minimum Protection Standards (MPS). (9) Removed Annex 1.4.6-2, Protectable Items. Refer to IRM 10.2.15, Minimum Protection Standards (MPS). (10) Added background to IRM 1.4.6.1, Scope and objectives of the programme. (11) Addition of authority to IRM 1.4.6.1, scope and objectives of the programme. (12) Addition of responsibilities to IRM 1.4.6.1, scope and objectives of the programme. (13) Addition of management and review to IRM 1.4.6.1, scope and objectives of the programme. (14) Added definitions and acronyms to IRM 1.4.6.1, scope and objectives of the programme. (15) Added IRM 1.4.6.6, Facility Access. (16) Added IRM 1.4.6.6.1, Access to unauthorized facilities. (17) Added IRM 1.4.6.6.2, Access to the escorted structure. (18) Revised identification (ID) Media requirements throughout the manual. For guidance on ID media policies, see IRM 10.2.5, Identification Media. (19) Revised requirements for physical access control (PAC) throughout the manual. For on PAC policies, see IRM 10.2.18, Physical Access Control (PAC). (20) Revised privacy and information protection requirements throughout this manual. For policy guidance, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy (21) If the section change date has changed, but the section is listed, so that section had minor changes, clarifications, name changes, updated hyperlinks, or other examples. (22) This IRM incorporates the provisional guidance FMSS-01-0418-0001 to clarify the professional series eligible for the issue of pocket implementation fees. Effect on other documents This IRM replaces IRM 1.4.6, Manager Safety Manual, dated August 2, 2016. Audience Servicewide Effective Date (05-04-2020) Richard L. Rodriguez Chief Facilities Management and Security Services This section contains the requirements of the head and security officer for the application and application of the IRS's minimum security standards. Purpose: This IRM section provides management and security officials with minimum security standards and flexibility to incorporate additional security measures needed to meet the needs of local geographic and demographic conditions and day-to-day operations for the entire federal tax administration administered within the IRS. Requirements for the protection of employees, facilities, equipment and infrastructure, as well as, tax returns, return information, cash, negotiable tools and other sensitive information and documents. Audience: Throughout the service. Policy Owner: Head, Management and Security Services (FMSS). Program Owner: Associate Director (AD), Security Policy. Main stakeholders: FMSS Field Operations, Business Unit Executives, Senior Managers, Chief Counsel Executives, Managers and Employees. Objectives of the program: To provide IRS managers and security officials with policies and procedures to enforce and enforce security standards. IRS security risks may vary in nature depending on the type, size, and location of a facility or operation. This guide has been developed to provide safety managers and officials with standard minimum safety requirements with flexibility to improve safety if necessary. Executive Order 13526, National Security Information The Privacy Act of 1974 Tax Reform Act of 1976 IRC 6103, 7213, 7217 and 7431 Federal Managers' Financial Integrity Act of 1982 (FMFIA) Government Accountability Office (GAO) Standards OMB Circular A–123 (Management) s Internal Control Responsibility) OMB Circular A-130 (Managing Information as a Strategic Resource) Treasury Security Manual 71–10 Federal Information Security Management Act of 2002 (FISMA) National Institute of Standards and Technology (NIST) SP 800-53 Rev. , FMSS prescribes and is responsible for overseeing the resource guidance policy of the manager safety manual. FMSS AD, Security Policy is responsible for supervising the and the development of the guidelines and resource guidelines of the Manager Safety Manual. The head of the FMSS Physical Security Protection Program (PSPP) section is responsible for planning, developing, implementing, evaluating, and controlling the policies and resource guidelines of the Managers Security Manual. IRS managers are for: Take all reasonable steps to prevent loss of life and property, disruption of services and functions, and unauthorized disclosure of documents and information to safeguard the continued functioning of the federal tax administration system. Apply compliance with the minimum security standards and policies contained in the field in which you are contained. Confirms that employees have knowledge and understanding of the roles and requirements of the Physical Security Program Consulting with FMSS Security Section Chief (SSC) for above-standard physical security countermeasures. Confirmation of the level of protection provided to prevent unauthorized disclosure of sensitive information is commensurate with the sensitivity level of the information. Confirmation of the level of protection offered to media containing the information is commensurate with the value of the media. Confirmation of the physical security measures necessary to protect life, information, property and all government assets are: i. applied within their supervisory area and ii. these measures meet the minimum safety standards set. Maintain effective controls to prevent fraud, waste or misuse of government resources and mismanagement of IRS programs. Control systems will provide a reasonable guarantee that all resources are protected from unauthorized uses or provisions. The basic standards and principles of the control system for all operators are: i. Documentation - Clearly written instructions for all financial transactions, resource accounting and internal control requirements will be readily available. ii. Liability - Transaction logs will be maintained and reviewed periodically for the purpose of determining whether transactions have been successfully authorized. Exceptions must be examined and corrective action taken. iii. Separation of duties - Duties such as authorisation, registration, issuing, receiving, reviewing and auditing or auditing will be assigned to separate persons to minimize the possibility that fraud, waste or abuse are not detected. iv. Supervision - Qualified and continuous supervision will be provided to ensure compliance with procedures. Periodic reviews will be conducted by managers. At. Access to resources - Direct physical access to resources and indirect access through the preparation or processing of documents will be limited to authorized personnel. Vi. Competent Warranty - Key staff are of high integrity and are competent based on education, training or experience to carry out their tasks. Reasonable assurance - Internal control systems will provide a reasonable that the objectives of the system are achieved. The cost of controls must not exceed the benefits. Viii. Breach Reporting - All managers will verify that potential breaches of internal control systems are reported quickly in accordance with established procedures. Verify that employees and comply with the security procedures established for the protection of information, documents, property and documents and for reporting loss, and any security breach to the competent authority. Verify that employees are trained to use physical security systems installed in their space as needed to help protect IRS resources. Program Reports: The authoritative source of data for monitoring the Manager Resource Guide, Managers Security Handbook will be: FMSS Physical Security Briefing Completion Reports Situation Awareness Management Center (SAMC) Program Effectiveness Report: FMSS PSPP Chief Section will evaluate the effectiveness of this program from: Evaluating the completion rate of all IRS employees for the mandatory annual Facilities Management and Security Services Physical Security Briefing located on ITM. Review and evaluate SAMC reports for safety incident trends. Controlled area - It is not a limited area; however, requires controlled access to the one-part authenticating input (access card or manual combination). Countermeasures: An action or device that can prevent or mitigate the effects of threats. Criminal Investigation (CI) - An IRS organization that is the law enforcement arm of the IRS with investigative jurisdiction. Employee - A federal employee employed by the IRS. Escorted access - A situation where a contractor employee has not yet granted similar access to staff who must be accompanied by a qualified escort during work performance and movement throughout the facility. Extended definition: A situation where an individual (e.g., contractor, visitor, or vendor) is not approved for personal access and requires escorted access. For more information, see IRM 10.23.2, Personnel Security, Contractor Investigations. Tree Access - Controlled entry into a structure based on access status, role or function, and category of use. Incident- Any event that affects the safety, safety or protection of property, a structure or occupant that requires a response, investigation or other follow-up. Limited Area - An area to which access is limited only to authorized personnel. Limited area space can be identified by the FMSS physical SSC based on critical resources. For more information, see IRM 10.2.14, Methods of Providing Protection. Qualified Escort - An authorized (designated) IRS employee or contractor employee approved for final staff-like access at the same level of position or higher risk as the contractor employee requesting escort and with knowledge of the task or to be executed. For more information about the escort/escorted ratio, see IRM 10.2.18.5.2, Escorted Access. Routine access - Access to facilities on a constant basis, usually several times a week. Security Section Chief (SSC) - An FMSS operations manager responsible for physical security within a region. Similar access to staff - - Unauthorized access to Treasury-owned structures, IT systems, products and security products and/or areas that store/process SBU data, as determined by Treasury/Office officials. Personal access may be temporary or permanent. For more information, see IRM 10.23.2, Personnel Security, Contractor Investigations. Unauthorized Access - Similar staff access granted to a contractor employee to unaccompanied IRS facilities, IT systems, and SBU data. Extended definition: Authority granted to individuals to gain access/entry and be present unescorted. Unauthorized access is a similar element of the access permission to staff. For more information, see IRM 10.23.2, Personnel Security, Contractor Investigations. Acronym Definition AD Associate Director DO Designated Official FMSS Facilities Management and Security Services FOIA Freedom of Information Act ISC Interagency Security Committee LOP Level of Protection SAMC Situational Awareness Management Center SBU Sensitive But Unclassified SSC Security Section Chief TDP Treasury Directive Publication TIGTA Treasury Inspector General for Tax Administration TM Territory Manager(s) VAR Visitor Access Register IRM 1.15, Records and Information Management IRM 10.2.1, Physical Security Program IRM 10.2.5, Identification Media IRM 10.2.6, Civil Enforcement and Non-Enforcement Pocket Commissions IRM 10.2.8, Incident Reporting IRM 10.2.11, Basic Physical Security Concepts IRM 10.5.1, Privacy and Information Protection, IRM Privacy Policy 10.5.2, Privacy and Information Protection, Privacy Compliance and Assurance (PCA) IRM Program 10.5.4, Privacy and Information Protection , Incident Management Program IRM 10.5.7 , Privacy and Information Protection, pseudonym use by IRS IRM 10.5.8 employees, Privacy and Information Protection, Sensitive but Unclassified Data Policy (SBU): Protecting SBU in Non-Production Environments IRM 10.8, Information Technology (IT) Security IRM 10.9.1, National Security Information IRM 11.3, Disclosure of Official Information A guiding principle of security within the IRS is to restrict access to resources as needed. When applied to information security, this results in restricting access to documents on a need-to-know basis. As for physical security, it means limiting entry to rooms, areas or facilities based on the duties or responsibilities of the individual. To maintain reasonable security at all IRS facilities at all times only authorized visitors will be allowed to enter the facility. It is not allowed to provide guided tours for interested, non-tax individuals or groups, or groups to guide them with Official visits by individual tax preparers, accountants, media representatives and other tax-oriented individuals and professional groups may be permitted at the discretion of the facility manager or senior representative (SCR), in coordination with communication and liaison (C&amp;L), local FMSS physical security personnel. For more information about restricting access control, see IRM 10.2.18, Physical Access Control (PAC). Determining the need to access information, documents, rooms, areas, or facilities is based on whether a person needs access to perform assigned tasks and responsibilities. Does the individual need to know? Should the individual enter a protected area? Management determines the need and subsequent decision to grant access to an asset. Consult your local FMSS physical security staff to select the appropriate means to get the desired access control. The warranties presented in this manual are designed to protect against such human threats as: acts of accidental violence/deliberate alteration or destruction of information or bomb threats owned demonstrations/riots fraud sabotage unauthorized theft disclosure vandalism unauthorized entry Protection methods are designed for the complete protection of IRS assets at all times. Security methods are also designed to restrict access by non-IRS individuals who may request access to IRS facilities. Because every single protection is often insufficient protection for any resource, the concept of securing security measures has been developed to ensure in-depth security. To understand security in depth, it is important to know what needs to be considered before choosing the appropriate protection, or combination of safeguards, necessary for a particular asset. The value of the asset and the applicable laws are the main considerations. Once determined, the issue of unauthorized access is resolved by one or all of these methods: Deter Detect Deny Delay Defend/Respond Ideally, physical security measures must provide a structure with absolute protection from a number of threats. While absolute protection is unattainable, a hands-on approach to physical security is essential to protect personnel, information, facilities, and property by employing a combination of measures to deter, detect, deny, delay, defend against unauthorized operators without being so restrictive that security itself becomes an interruption. Management: Verifying information such as training materials, statistical files, and various internal communications that require undesirable dissemination and dissemination is protected. Determine the required level of protection, based on policy requirements. Work with FMSS physical security personnel to implement appropriate security measures. Verify that the are trained to use physical security systems installed in their space, if necessary, to help protect IRS assets. The Minimum Security Standards (MPS) system establishes a uniform method for protecting resources that require protection. The MPS system is designed to provide managers with basic framework of minimum physical safety requirements with flexibility to address local conditions. For more information, see IRM 10.2.15, Minimum Protection Standards (MPS), and IRM 10.2.11, Basic Physical Security Concepts. Security must be addressed whenever the IRS space is designed, captured, modified, or redesigned. Failure to consider adequate security during the early stages of space planning can result in costly changes. Further information on space design and planning is described in the IRS's national standards. For more information, see IRM 10.2.11, Basic Physical Security Concepts. The designation of a limited area is a method of controlling the movement of people and eliminating unnecessary traffic through critical security areas, thus reducing the risk of unauthorized disclosure or theft of tax information. Limited area space can be identified by the FMSS physical SSC based on critical resources. All restricted areas must meet protected area requirements. For more information about restricted areas, see IRM 10.2.11, Basic Physical Security Concepts. Protected areas are designed to prevent undetected entry by unauthorized persons. Local physical security specialist FMSS will help determine the best method to meet minimum security standards for protected area/perimeter security. For more information, see IRM 10.2.15, Minimum Protection Standards (MPS). A controlled zone requires controlled access with authentication in one part (access card or manual combination). Only authorized personnel and other personnel designated by the responsible business unit are allowed to enter without access to a controlled area. All visitors entering a controlled area must be accompanied by personnel with unauthorized unauthorized access to that controlled area. Controlled areas include, but are not limited to: Central Security Control Console (CSCC) Alarm panel room/cabinet other similar structures designated for access controlled by the responsible business unit For more information about access for a controlled area, see IRM 10.2.18, Physical Access Control (PAC). Keys, key cards and block combinations are a means of controlling access. If the key, key, or combination is not strictly controlled or compromised, physical security is lost. For more information, see IRM 10.2.14, Methods of Providing Protection Local on-site FMSS physical protection personnel will keep keys for the IRS space, in case of inadvertent office locks. Replacement keys can be from an off-site business function designated for use in catastrophic situations where local staff are available to provide access to the IRS space. No more than two keys are allowed for each FMSS budget lock mechanism for and maintenance funds and replacement of office access controls, locks and keys. Security combinations the storage of classified NIS must be protected at the level of the information stored in the containers. This includes ensuring that combinations are never discussed outside a safe area, that they are never written, and that combinations are modified by an authorized and informed employee when individuals who had access no longer require it. For more information, see IRM 10.9.1, National Security Information. The criminal investigation (CI) will maintain its key and combination control, complying with the above standards, except that no approval for duplicate keys by local physical security personnel is required and control of SF 700 will remain in CI. Information protection is a vital issue for the IRS. All IRS employees who have access to tax returns or return and privacy information are prohibited by the statute from disclosing official information, except as authorized by applicable law or regulation. Information security includes information stored on handheld communication devices, external storage devices, computers, laptops, or paper documents. In addition to tax data there are many other documents that require disclosure protection. For more information, see IRM 11.3, Disclosure of Official Information. Protecting the information discussed in this section is vital to the IRS business, however, it should not be confused with classified NIS. For more information, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy. The Privacy Act of 1974, 5 USC 552a, provides full legal recognition of an individual's right to privacy. Recorded information that is retrieved by reference to a name or other personal identifier, such as a Social Security number, is privacy information. The act specifies that agencies will establish appropriate administrative, technical, and physical safeguards to ensure document security and protect records from any threats or threats to their security or integrity that could cause substantial harm, embarrassment, inconvenience, or injustice is to any individual on whom the information is maintained. For more information, see IRM 11.3.14, Privacy Act General Provisions. Disclosure of information must be reported to Privacy, Government Liaison, and Disclosure (PGLD) in accordance with IRM 10.5.4, Privacy and Information Protection, Incident Management Program. People who provide information about tax violations expect and deserve to have their identity protected. All employees must therefore manage information in close trust. In order to maintain maximum security, whistleblower communications, reward requests, reward reports, memoranda or other documents identifying whistleblowers will always be protected, except when such documents are processed. Access to such storage containers will be restricted person/persons responsible for the security of documents. For more information, see IRM 25.2, Information and Whistleblower Awards. Classified NSI is any information, regardless of form, relating to U.S. national defense or foreign relations, which is owned, produced by/for, or is under the control of the U.S. government and, if not adequately protected, could cause harm to national security. Executive Order 13526, Classified Information on National Security, or Substitution, prescribes a uniform system for classifying, safeguarding, and declassifying national security information. NSI, commonly referred to as classified information, is information that requires protection against unauthorized disclosure and must be accessible only by those who have an authorization to or above the information to access, a need to know to perform their functions, and a signed SF-312, agreement of non-disclosure of classified information. NSI is marked As Secret, Secret, or Confidential to indicate its need for protection regardless of the form it is in. NSI must be transported in a particular way and cannot be processed on unclassified systems, it must also be destroyed using the latest Shrew of the National Security Agency/Central Security Service (NSA/CSS) Evaluated Products List (EPL). For more information, see IRM 10.9.1, National Security Information. SBU data is all information that, in the event of loss, theft, misuse or access or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations) or the privacy to which people are entitled under the Privacy Act. Real-time data, defined as production data in use. Live means that when you change the data, it changes in the production environment. The data can be extracted for testing, development, etc., in which case, it is no longer live. Real-time data often contains SBU data (including personal information and tax information); however, tax information (FTI) remains tax information (FTI) whether it is a production environment or a non-production environment. For more information, see IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments. Documents and documents created or received by the IRS in connection with operational and administrative activities are official information and owned by the U.S. government. In accordance with 18 USC 2071, Concealment, Removal or Mutilation In general, it is illegal to remove documents from IRS custody, except in accordance with the prescribed procedures. The Tax Reform Act of 1976 requires that return and return information be confidential and not subject to disclosure, except as specifically specified in IRC 6103, confidentiality and disclosure of return and return information, or other sections of the Internal Revenue Code. For more information, see IRM 1.15.1, Records and Information Management, The Records and Information Management Program. A large volume of IRS activities, such as tax returns, remittances, and government controls, are transmitted by mail. Unattended mail is an easy target for theft. Mail, unde deployed or processed, must be: stored in a protected area or in locked containers. not left unattended in areas open to the public. For more information, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy, and IRM 1.22.5, Mail and Transportation Management, Mail Operations. Field employees can sometimes have sensitive and/or personally identifiable information (PII) at the taxpayer's location (position where the taxpayer conducts corporate or hosted tax information). Because it is not always possible to remove information from the taxpayer's site and store it at an IRS facility, executives must confirm that employees understand the importance of protecting that information at the taxpayer's site in a locked container when not in use. Sensitive tax information, such as agent work documents, original declarations, examination plans, fraud data, etc., which is hosted at a taxpayer's site, must be stored in a security container under the control of the responsible employee. The taxpayer cannot have access to this container. The data will not be stored on the taxpayer's premises during non-service hours if a security container is not available. During service hours, data must be in the employee's personal custody when it is not contained. Personal custody exists when an employee responsible for the IRS or another designated person (e.g., armored car service employee, authorized employee of a contract company) has possession or eye contact with a document or property element. For the purposes of this definition, eye contact is limited to the person's desk or the immediate workspace over which he or she has physical control. For more information, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy, and IRM 10.2.15, Minimum Protection Standards (MPS). During official travel it is often necessary for to carry tax data, laptops, taxpayer checks and money orders, etc. Employees are responsible for the loss, theft, or disappearance of IRS assets when they are attributable to negligence. Employees in custody of sensitive information or IRS property outside an IRS office must protect such items to the greatest extent possible. For more information, see IRM 10.5.1, 10.5.1. and Information Protection, Privacy Policy. The IRS regularly ships tax returns and returns information between IRS locations, as well as other federal and state agencies. Data in transit is particularly vulnerable to loss, destruction and disclosure. Such a loss could cause irreparable harm to the government or taxpayers, delay tax treatment, and damage the Public Image of the IRS. All tax return shipments and return information from any processing or processing center, area office, service posts, or other agencies and jurisdictions must be documented and monitored to safeguard liability and receipt for each shipment. For more information, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy. The purpose of destroying waste material generated in the processing of tax documents or other related documents is to prevent information from being disclosed to unauthorized personnel. The provision and destruction of tax information must comply with IRM 1.15.2, Log and Information Management, Document Types and related lifecycles. To improve the level of protection provided with tax and privacy data, the IRS has adopted a clean desk policy. The goals of IRS Clean Desk Policy and containerization are designed to address SBU data protection (including personal information and tax information) throughout the privacy lifecycle. Clean Desk Policy requirements apply to data left out in workspaces (including workspaces and out-of-office) and unprotected containers, on beliefs, desktops, fax machines/copiers, meeting rooms, and in/out bins. All SBU data (including personal and tax information) in unprotected areas must be containerized during non-service hours. For some pipeline tasks and processing conducted at dispatch processing centers, campuses, and compute centers, the volume of tax information processed and the interruption of these operations could prevent the containerization and implementation of Clean Desk. For more information, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy. A security program is most effective when all managers and employees are aware of security requirements, including the reasons for each security requirement they must follow or enforce. Security awareness is promoted by the attitudes and actions of managers. If managers can explain security requirements in various situations and show how these requirements apply to their workspace, employees usually accept the need as part responsibilities. The management will implement a security awareness program and include: ITM Physical Security Mandatory Briefing. security as a regular topic in regular management meetings. safety guidance for all new employees within the first seven working days of employment. All seasonal employees will be given an update orientation the first seven working days or if they have been out of work for at least nine months. Local management will determine who will provide the guidance. recurrent safety briefing sessions conducted throughout the year by all processing/processing center supervisors. Safety briefing sessions will also be provided at the beginning of each storage season. a briefing to each employee of special security requirements related to their particular workspace within 30 business days of hiring. Plans must be made to properly protect and account for all tax data and other information, as well as government ownership when an office moves to another location. The circumstances of the move must be carefully considered (e.g. the distance and method to be used to make the move). Tax documents and other sensitive information must be stored in closed cabinets or sealed in packaging cartons during transit. For more information, see IRM 10.5.1, Privacy and Information Protection, Privacy Policy. The federal tax administration system is critical to the U.S. economy and must be protected at all times. To provide adequate protection, it is necessary to develop policies, plans and procedures that reduce the effect of accidents and emergencies. Accidents and emergencies are any situation or condition at global, national or local level that threatens or has the potential to threaten the safety of employees, information, systems, equipment, facilities and/or infrastructure. For more information, see IRM 10.2.9, Occupant Emergency Planning. Timely incident reporting is essential to advise all levels of condition management that affect the functioning of the IRS. Analyzing these trends or patterns detected will help an effective development of countermeasures to minimize the effect of future outages. Employees will contact one of the following offices to report an incident based on what has been lost, stolen, or disclosed: Privacy, Government Link, and Disclosure Incident Management Office. If the breach results in unintentional unauthorized disclosure of SBU data, including personal information and tax information, which is not taxpayer correspondence (see OTC in IRM 1.4.6.4.1 (3) b), such as verbal disclosure, or electronic disclosure such as SBU or PII or FTI data in an IRM section, Training Materials, PowerPoint, IRWeb, real-time test data uploaded to a system, etc., or lost/stolen or stolen paper documents or documents, or lost/stolen packages during UPS or FedEx shipping, or remittances report to PGLD/IM using the pII Breach Reporting Form. The Taxpayer's Office of Correspondence. If the breach concerns taxpayer correspondence generated in one of the following formats: notices, letters, transcripts, faxes, EEFax and other electronic transmissions such as e-mail, report it to the OTC using the Erroneous Taxpayer Correspondence Reporting Form Information Program (SNIP) Notice. The Center responds to computer security incidents (CSIRC). If the incident/violation results in the loss or theft of an IRS IT asset, such as an IRS-issued computer, laptop, router, printer, mobile phone, BlackBerry, etc., or removable media (CD/DVD, flash drive, floppy, etc.) or a provided/personal non-governmental mobile device that accesses, processes, transmits or stores IRS information, in support of the Bring Your Own Device (BYOD) program, report it to the CSIRC using the computer's security incident reporting module or by calling CSIRC at 240-613-3606. The Situational Awareness Management Center (SAMC). If the incident involved lost or stolen Smart-ID cards or lost or stolen pocket fees (credentials), report it to SAMC (within 30 minutes) using the SAMC Incident Reporting Link and selecting the Report a New Physical Incident button. The Inspector General of the Treasury for Tax Administration. If the incident/violation results in loss or theft (including BYOD devices), report it to TIGTA at 800-366-4484. For more information, see IRM 10.2.8, Incident Reporting. Occupant contingency plans (OEPs) are an essential part of a safety programme. Properly developed plans can reduce the threat to staff, property, and other resources, minimizing work disruption. GSA requires an OEP for all spaces occupied at the federal level. If the IRS is the main agency of the occupiers (the agency with the largest population in the facility) the designated official will develop, maintain and test the occupants' condency plan. The designated official is the highest official of the primary occupying agency. Emergency situations must be addressed so that staff know what procedures to follow. Typical situations and incidents included in the OEP are: bomb threats, explosions, demonstrations, Shelter in Place (SIP), utility outages or failures, natural disasters, disturbance weather conditions, fires, accidents, Adam/Amber Code, Active Threats, etc. For more information, see IRM 10.2.9, Occupant Emergency Planning. A continuity plan is a guide to re-establishing operations in order after an accident. The goal of the plan is to resume processing critical functions as quickly as possible and finally resume normal operations. A properly developed continuity plan requires coordination with all IRS organizations located at the facility. Each function will participate in the development of the plan by identifying critical needs (e.g. critical needs of staff and etc.) and will assign staff to participate in the planning process. Emergency management planning must include the recovery of critical information systems, vital registries, telecommunications, security, environmental concerns and the facility that hosts the working environment. For more guidance, see IRM IRM Business Continuity, Continuity Planning Overview, and IRM 1.15.2, Records and Information Management, Record Types, and Their Lifecycles When Planning and Developing Continuity of Operations for Vital Records, considered essential for the IRS to continue to operate before, during, and after an emergency or emergency. The authorized forms of identity media approved for use by IRS employees, contractors, and visitors are as follows: identity cards (photo and non-photo) as prescribed in IRM 10.2.5, Identification Media. Pocket commissions for civil application and non-application, as required by IRM 10.2.6, commissions for civil application and non-application. Enforcement Pocket Commissions as prescribed in IRM 9.11.3, Tax and Personnel Matters, Investigative Property. Parking permits for parking areas controlled by the IRS. Insignia provided IRS personnel with attachment to the issued clothing. For more information, see IRM 10.2.5, Identification Media. Authorized photo ID cards are SmartID and Physical Access Card (PAC). SmartIDs can be issued to people who meet personal access eligibility requirements and require routine access to IRS-controlled facilities and/or information systems. PAC cards can be issued to people who meet personal access eligibility requirements and require routine access only to IRS-controlled facilities. The SmartID will be worn over the employee's waist (on the torso) with the photo clearly visible from the front while in the IRS facilities. Smartids must be transported to an IRS-issued holder to safeguard the ID certificate. All ID cards must be retrieved by employees who separate from the IRS. For more information, see IRM 10.2.5, Identification Media. Visitors and federal or non-federal personnel who have met personal access eligibility requirements as set forth in IRM 10.2.18, Physical Access Control (PAC) will be issued non-photo Visitor ID cards by local FMSS Physical Security staff for unauthorized access. Non-photographic ID cards are issued by local FMSS Physical Security personnel to: Visitors, to include federal and non-federal personnel who have met the eligibility requirements for similar access to personnel, as set out in IRM 10.2.18, Physical Access Control (PAC). Visitors, to include contractors and federal or non-federal personnel who did not meet the eligibility requirements for personal access. These IDENTITY cards will be clearly as ESCORT ONLY. Employees reporting to IRS facilities without their photo ID card. Visitors who have not met the eligibility requirements must: be accompanied by an IRS employee, who must apply for his placement on the property's visitor access list. present a valid identity card for the identity verification card and undergo the screening procedures for the entrance of the structure. a non-photographic identity card Only Visitor Escort. Non-photographic photo ID cards be removed from the issuing facility and should never be used as an access permission to a facility. Non-photographic IDENTITY cards must be returned to local FMSS physical security personnel or to the guard post by the person to whom the card is assigned when the individual leaves the facility or security area. Identity cards for the non-photographic limited area are issued by designated limited area business unit monitors. Pocket commissions are used to present proof of authority in the performance of official tasks. They are primarily intended to identify IRS staff to the public when it comes to tax matters and cannot be issued just to identify employees for the routine activity transaction. There are three categories of pocket fees: application, civil application and non-execution. Enforcement fees are issued only to persons in a series of criminal investigations 1811. Civil enforcement and non-execution fees are issued to all other authorized employees. For more information, see IRM 10.2.6, Civil Enforcement and Non-Enforcement Pocket Commissions. Section 3706 of the IRS Restructuring and Reform Act of 1998 (RRA 98) of 26 USC 7804, dated July 22, 1998, provides that any internal revenue service employee may use a pseudonym only if the employee provides adequate justification for the use of a pseudonym, including the protection of personal safety; This usage is approved by the employee's supervisor before the pseudonym is used. The verbatim text of Section 3706 of IRS RRA 98 is set out in Annex 10.5.7-1, Verbatim Text of Section 3706 (RRA 98) from 26 USC 7804, dated 22 July 1998. Your PC and smartID must contain the same name, legal or pseudonym. The SmartID must be obtained before the PC. No employee can have more than one SmartID or active PC in their possession. If an employee is released a PC using a registered pseudonym, that individual cannot be released any other PC. If an employee already has a PC, the employee manager must retrieve the PC before a PC is released under a pseudonym and return it to the PC team using shipping requirements. The same process applies to issuing a PC under a pseudonym. A PC released under a registered pseudonym cannot be used as a retirement memory, for an honorary presentation, or for similar purposes. A registered pseudonym PC owner cannot be reissued a PC in their legal name for remembrance purposes. Your PC must be retrieved by the employee manager and sent to the PC team for destruction. for more information click to IRM 10.5.7, Privacy and Information Protection, Use of Pseudonyms by IRS Employees. Access to IRS facilities and workspaces is provided to IRS employees, contractors, and visitors on a escorted or un escorted basis. The local FMSS physical security office will determine and grant the type of access, based on eligibility All persons entering or requesting access to a government building are subject to the provisions of the rules and regulations governing buildings and public land. This includes the Federal Management Regulation (FMR), Title 41, the Code of Federal Regulations (CFR); Part 102-74, Subpart C Conduct on Federal Property and Title 18, United States Code (USC), Section 930, Possession of firearms and dangerous weapons in federal facilities. For more information, see IRM 10.2.18, Physical Access Control (PAC). Only employees, IRS contractors, other employees, and contractors from federal agencies that meet eligibility requirements are allowed access without access to IRS facilities. Non-federal personnel who meet eligibility requirements can be issued a physical access card (PAC) for use in that facility, after a favorable judgment for personal access. The non-photographic IDENTITY cards issued must not be removed from the issuing facility. Contractors, 300 of them, who do not have an ID card for photos issued by the IRS, can be placed on a VAR, approved by the local FMSS physical security office. For more information, see IRM 10.2.18, Physical Access Control (PAC). IRS contractors, other federal agency employees, and contractors and visitors who do not meet the requirements for unaccompanied access must be escorted at all times while in the IRS facilities and workspace. Escorted access does not allow entry and/or movement throughout the property without a qualified escort. Escorted people require a qualified escort. Qualified escort requirements are authorized (designated) IRS or contracting employees approved for final access similar to personnel at the same level of position or higher risk as the escorted person. Authorized employees and contractors who require routine access to IRS-controlled facilities with an electronic access control system can be issued an access card to the facility, also known as a proxy card, where necessary. Employees requesting a proxy card must fill out and submit Form 13716, Request for ID Media and/or Access Card for IRS employees, to local FMSS physical security personnel to obtain their proxy card. The IRS has established minimum standards and requirements that IRS leaders must safeguard. Recurrent assessments and reviews help security personnel and management officers determine the effectiveness and adequacy of existing security warranties and guidelines. Functional reviews measure compliance with security policies and that apply to each manager's office or functional area. Functional reviews allow managers to verify that existing security policies and procedures are followed daily. Frontline managers must conduct functional reviews at least on an annual basis or more frequently depending on the security requirements of their business unit. The review must be documented in form 12149 and and the reviewer must provide a copy of the report at the next management level. Review policies may be based on local concerns, but managers should assess their area on: Clean Desk Policy Disposition of waste material ID Media Locks and keys Protection of sensitive information Security awareness An after-hours review allows managers to determine whether assets are adequately protected when they are not in the custody of authorized IRS personnel. Managers can do this by checking the area after the daylight is closed or before the facility is opened to verify workspace compliance. Managers: Periodically review functional areas after working hours to determine whether sensitive information is adequately contained, disposed of, whether cabinets, safes, and other containers are adequately protected, and whether restricted areas, safe areas, and office doors meet security requirements. take immediate measures for identified weaknesses to safeguard information, assets or premises/facilities, advise employees as appropriate and/or request assistance from the local FMSS SSC to develop corrective measures. Contracts for services or goods involving the disclosure of sensitive information to a contractor (e.g. return or return information, personnel information, and administrative or internal management information critical to the IRS mission), must include appropriate protection measures in accordance with applicable laws, regulations, and procedures. IT Cybersecurity and FMSS, can assist in the review and provide their respective skills. Refer to Guidelines for managing service-level records for contractor records. Managers confirm that requests for contractual services involving the disclosure of sensitive information are reviewed by PGLD and, where appropriate, IT Cybersecurity, as well as FMSS Physical Security. Managers consult with FMSS physical security personnel to determine the detection and security requirements of the contractor's site. For automated information services, see IRM 10.8.1, Information Technology (IT) Security, Policy, and Guidance. An existing contractor's ability to adequately protect IRS data from unauthorized uses or communications must be recertified annually for contracts that extend beyond a period of one year, prior to the renewal of the contract, or if the warranties used by the contractor become a matter of concern (e.g. suspected security breach). Contact the Office of Privacy, Government Liaison and Disclosure Incident Management if recertification due to a disclosure issue to inform them about the concern. The contractor will be required to provide a self-assessment regarding their ability to protect IRS data. If you cannot determine the recertification status from self-assessment and other documentation, you must schedule the review of the recertification site of the contracting structure. Due to regulatory requirements, the security of the IRS (Cybersecurity and/or FMSS) may Site reviews each year depending on the nature of the issue (for example, Federal Information Security Management Act (FISMA), see Pub. 4812, Contractor Security Controls). Manual of additional internal revenue