Corporate Procedure 10.13

Asset Protection:

Normal & Sensitive Parts Security

Document Number CP10.13

Version 9

07/29/2013

Document Owner: Integrated Supply Chain

Asset Protection Competency Center

Table of Contents

Preface

i. Summary of Changes

Edition #	Edition Date	Nature of Change	Revision Tag	Date Approved
N/A	12/14/91	N/A	N/A	12/14/91
Version 1	6/10/94	Rewrite in full	N/A	6/10/94
Version 2	2/06/95	Re-release	N/A	2/06/95
Version 3	7/30/96	Re-Release	N/A	7/30/96
Version 4	7/14/2000	Re-Release	N/A	07/28/2000
Version 5	12/12/2003	Removal of APC 5 Redefined APC 3 Removed Machine requirements	N/A	12/12/2003
Version 6	12/12/2006	Loss Reporting Classification of FFBM Updated SOD requirements	N/A	12/12/2006
Version 7	04/15/2008	Incorporation of CS 1-1121-016, due to removal of Corp. Specification	N/A	04/24/2008
Version 8	09/16/2010	Changed APC3 classification criteria and control requirements, all sections. Changed SPD parts validation to annual. Large Assemblies can be stored outside vaults. Added the data retention for CCTV's. Eliminated the requirement to use the Loss Incident Tracking Database. Clarified the final disposition for APC-4 parts.	N/A	12/09/2010
Version 9	07/29/13	Re-Write • Format Change • Removed Section 4.7 & 4.8 • Defined Vendor/BP requirements	N/A	09/04/13

ii. Document Change Approvers

The following must review and approve any changes:

- Integration Supply Chain Manager and Global Operations

This is an approved document. It replaces Corporate Procedure 10.13 dated 09/16/2010

iii. Document Approvals

Document approval for this document is maintained by the author.

iv. Document Review Plans

This document will be reviewed and updated as necessary.

v. Document Owner

This document is owned by Global Operations. The author is the Asset Protection Competency Center, Lotus Notes - "Asset Protection Help Desk/Endicott/IBM@IBMUS" or E-Mail "DACS@us.ibm.com". The source document is kept online.

vi. Document Distribution/Access

The current released level of this document is available online at:
http://w3.ibm.com/ibm/resource/isc_gl_asset_protection.html#Asset_Protection

1.0 Introduction

1.1 Scope

The objective of this Procedure is to ensure the security of IBM parts and IBM owned machines. This Procedure establishes standard IBM requirements for the classification, security, protection, control and disposition of normal, and sensitive parts and IBM controlled machines. This Procedure covers the security of all parts and finished goods, regardless of usage, from the inception of the part in the development cycle through the parts end-of-life cycle, end of maintenance and final disposition.

1.2 Asset Protection Initiatives

IBM's management, employees, subsidiaries, Business Partners and Suppliers have the responsibility for assuring attainment of the Asset Protection Initiatives, which are:

- Assure the preservation IBM revenue through proper asset controls.
- Assure parts disposition in a manner preserving IBM's quality reputation.
- Assure asset protection decisions provide benefit to the IBM Company.

1.3 Applicability

The provisions of this Procedure are corporate-wide in application including subsidiaries, Business Partners, and Suppliers. The contract owner is responsible to ensure that supplier contracts address all the requirements to protect IBM assets and interests as prescribed by the process owner. There are no exceptions to the intent. However, every situation cannot be covered relative to the security and protection of parts and hardware. Judgment will be required when applying these instructions to specific conditions; when properly applied, deviations will not be created. In cases of doubt, the organization's designated Asset Protection Peer Council Representative, as well as other support organizations, should be consulted for advice and guidance.

1.4 Organization Responsibilities

Asset Protection Competency Center (APCC)

The APCC is responsible for establishing the strategy and framework for the corporation on asset protection as well as develop worldwide asset protection programs and systems. Other responsibilities include:

- Assure the corporate intent is implemented and effective.
- Interface with corporate staffs and Business Units on practices, controls, and other related aspects of the asset protection program.
- Provide advice and guidance through the appropriate functional units.
- Provide guidance/assistance to the operational units as required.

Asset Protection System Administrator

- Administer a corporate Sensitive Parts Database (SPD) containing asset sensitive part information.
- Provide controlled access and update capability to Sensitive Parts Administrators within the units.
- Ensure the responsible SPA completes the annual validation of parts in the SPD.

Central Asset Tracking System (CATS) – Application Owner

The application owner maintains the responsibility for defining the systems requirements and for operational, maintenance and development activities. These responsibilities are delegated to the Asset Protection Competency Center.

Business Units (Groups / Divisions / Geography's)

Each Business Unit will identify individuals and develop processes to assure proper implementation / deployment throughout the respective organizations. Additionally each Unit must have a management process which will ensure the proper level of management focus to assure compliance to the requirements of this document.

Each Business Unit will also define the support structure that will facilitate the implementation of the following activities:

- Assign an Asset Protection Peer Council (APPC) Representative to be the conduit for asset protection information between the APPC and the Business Unit. The representative is responsible for ensuring that the unit executives are kept aware of the current status of asset protection initiatives. This individual will organize an extended peer council (as required) with cross functional representation within the unit, to ensure that asset protection information is communicated to and properly deployed by the organization's operational units.
- Identify a Sensitive Parts Coordinator to develop and implement a parts security program with practices consistent with the requirements of this procedure. Additional monitoring and self-assessment activities must be implemented to ensure program adequacy, process compliance and management awareness.
- Establish and identify the Sensitive Parts Administrators (SPA and backup) who will function as the unit's single focal point for sensitive parts administration, as required. The SPA is responsible for maintaining the sensitive parts profiles for the unit and ensuring the information in the Sensitive Parts Database (SPD) is accurate and current.

Asset Protection Peer Council (APPC)

The Asset Protection Peer Council was established to communicate/share information on asset protection throughout the corporation. It is intended to do this via periodic meetings and publications. The membership is comprised of representatives from Business Units, geography's, and CHQ support organizations.

Macro-Point Responsibilities

- Each Business Unit will define its tracking points (Macro-Points) where data will be recorded and sent to the Central Asset Tracking System (CATS).
- Each Business Unit must develop a process and/or systems to perform the tracking activities.
- All Macro-Point transactions must be recorded within 1 business day of the tracking event and promptly reported to CATS. It is a critical requirement that this data be of high quality and integrity and provide an audit trail to the business process.
- A management process must exist in each Macro-Point to ensure the proper level of management focus for tracking compliance.
- Parts must also be tracked through all transfer activities between Macro-points.
- Each Business Unit must define and implement a tracking practice for APC 4 parts handled by a supplier.
- Each Macro-Point is required to maintain the following roles.
    - Macro-Point Management Contact
        - Receives weekly management awareness reports from CATS on tracking activities.
        - Responsible to ensure appropriate actions are being taken by the Administrative Contact
    - Macro-Point Administrative Contact
        - Receives daily activity reports from CATS on tracking activities.
        - Responsible for all tracking transactions for the Macro-Point and first point of contact.

2.0 Sensitive Parts

2.1 Sensitive Parts Identification and Process Responsibility

Asset sensitivity decisions are made at the part number level. The Development Organization releasing a part number has the initial responsibility to evaluate the asset sensitivity in the product development cycle and assign the asset protection classifications as appropriate. This includes engineering prototype parts. The Classification process starts at the Develop Phase and continues through the Life Cycle of the part and the products in which it is used. The on going sensitive part classification is the responsibility of the Unit of Control. Each Unit of Control will determine and document its criteria for classifying a part as sensitive, as well as the level of classification.

Notes:

- The process to classify a higher assembly is not an automatic decision based on the highest classification of the parts in its structure. It must take into consideration the asset sensitivity of each part in the assembly's bill of material, as well as the asset or technology sensitivity of the higher assembly itself.
- Interchangeable parts with different part numbers (Manufacturing P/N, Field Replaceable Unit P/N, Card Assembly P/N, Options, etc.) must have equal APC values assigned at all times.
- The APC 4 part contained within kits must be consumed in CATS .
- Unit of Control handling regulated parts may have unique security plans for their sensitive parts management.

2.2 Sensitive Parts Definition

A part may be classified as sensitive for one or more of the following reasons:

- Technology - part has IBM proprietary technology or intellectual property that provides IBM a competitive advantage.
- Asset Value - part has high probable risk for loss or theft, has significant value/demand; has high recoverable/reuse value; has high market value; has the potential to displace IBM revenue/incur additional costs, if misappropriated.
- Business Unit defined requirements by taking into account some of the following points:
    - the market value of the part
    - the reuse value or recoverable value of the part
    - the potential to displace IBM/business unit revenue, (marketability outside IBM)
    - the potential for theft
    - the potential for fraud if misappropriated
    - the commodity family of the part
    - the liability to Legal and Regulatory requirements

Sensitive parts will have unique requirements, based on their level of classification that may include:

- unique inventory controls
- physical security part number/quantity control and reconciliation
- part number/serial number control and reconciliation
- central reporting of data and/or transactions
- a protected disposition

2.3 Asset Protection Classification (APC)

The Asset Protection Classification is a numerical identifier assigned to a part number that represents the degree of sensitivity. The Asset Protection Classification also determines the control requirements for the part number. IBM part numbers not defined within the Sensitive Parts Database are assigned an Asset Protection Classification of zero (0), non-sensitive.

The following criteria are to be used as suggested primary guidelines for determining the asset protection classification of a part.

APC = 0:

Are not considered sensitive parts.

APC = 1:

A part that has value and as such requires a protected disposition. APC 1 parts are not considered sensitive.

APC = 2:

A part that has a high market demand / value and a risk for theft or loss either individually or in volume and having at least three of the following characteristics:

- Readily sold (marketable)
- History of frequent loss
- Easily carried by one person or concealed with little difficulty
- Attractive to acquire for personal use

Other items to be considered in determining classification may include:

- Potential impact to future service revenue
- History of part/commodity, including thefts and fraud
- High material recovery value
- Liability to legal and regulatory requirements

APC = 3:

Loss or misappropriation of parts in this category could have significant impact on business unit revenue.

General guidelines are:

- A part that has high risk for theft or fraud.
- Liability to legal and regulatory requirements.
- A part that has technical sensitivity and/or high market value but whose use is otherwise restricted by software or hardware license keys, integrated Vital Product Data (VPD), or some other asset protection method.
- A part that requires Tracking Identification Number (TIN) labeling.

APC = 4:

- A part that has extremely high value to IBM, and as such, requires TIN accountability via point to point tracking.
- Liability to legal and regulatory requirements.
- A part where the loss of proprietary technology or limited-quantity technology would cause IBM to lose a competitive advantage from disclosure of the technology or risk to IBM in the marketplace.

APC = 9:

A part number that is not sensitive and does not require controlled disposition but has strategic and/or economic value to the IBM Service Organization. The tracking requirements will be defined by the Service Organization at a local level.

2.4 Part Identification Labeling Requirements

All sensitive parts must be properly labeled with the appropriate label. The tracking identification applied to a part must meet the following Automatic Identification (AI) formats as defined in Corporate Standard, CS 1-1121-015 and Global Labeling Program.

It is the responsibility of each unit handling trackable sensitive parts that they are labeled with the approved format TIN, and that these parts do not move throughout the IBM logistics processes without the required tracking identification and tracking transactions.

- For parts in the IBM field inventory without the proper labeling, a TIN using one of the approved formats will be affixed to the FRU package. Labeling of the parts will be as agreed to by the manufacturing unit of control and the geographic service organizations.
- Questions on labeling of a specific part should be directed to the appropriate manufacturing location with reference to the Global Labeling Program.

FRU Packaging

To facilitate the tracking of IBM service inventory, in instances where the part (APC = 4) is also a FRU, a bar coded label with the FRU part number and TIN number (in 11S format) must be on the outside of the package, as well as the human readable FRU part number. The FRU TIN label on the box must be identical to the TIN labeling on the part. If there are numerous TIN labels on the part, the FRU TIN must be identified by adding the word 'FRU' in human readable format.

2.5 Sensitive Parts Database (SPD)

The Sensitive Parts Database (SPD) is the primary source for access to and communication of sensitive part information. Specific sensitive part information is entered into the SPD by completing the Sensitive Part Profile. The Unit SPA is responsible for the accuracy of the SPD.

The SPD is corporate-wide tool and is available to IBM units (read only) to enable them to implement the required controls for sensitive parts. It is the responsibility of each unit to integrate the information contained in the SPD into their logistics processes as applicable. On a weekly basis, information from the SPD is distributed to the requesting units with a business need, including any strategic suppliers, to receive this information. The SPD is limited to those with a "need to know".

At least once per year, each sensitive part will have its classification validated by the Sensitive Parts Administrator of the Unit of Control to assess that the conditions/criteria that initially warranted the classification level has not changed. It is the responsibility of IBM Development LOEC, IBM Global Service (IGS), IBM Global Finance (IGF) and Global Asset Recovery Services (GARS) to assist in identifying asset sensitive parts by communicating the market value and/or service value attributes of the parts, as necessary, to the Sensitive Parts Administrator of the unit of control for proper classification for the life of the part.

Note:

The APC Value in Product Manager / Enovia reflects the classification of the part number at release. This APC value in Product Manager / Enovia is not updated upon subsequent reclassification of the part number.

3.0 Asset Security IBM

IBM Security provides advice and counsel for security programs and practices. Business Unit management should consult with local security on unexplained losses for advice regarding whether a theft may have occurred. This process requires management to report thefts and suspected thefts in a timely manner per local procedure. Security and Business Controls can serve as a resource for advice on the completeness of Asset Protection programs and for assistance in detecting exposures in processes.

3.1 Physical Security

Refer to the IBM Security Manual for further details on physical security requirements for IBM locations and sites. Below are the minimal requirements for physically securing sensitive parts and physical assets. Ref. SECMAN PS02

Baseline Security - APC = 0, 1: Non-Sensitive Parts

Parts, physical assets and IBM owned machine must be protected in a locked enclosed environment, with access limited to management approved personnel. The following controls are required.

- Minimize entry and exit points.
- Windows on the ground floor where parts are stored must be:
    - Inoperable and/or locked
    - Screened in such a manner as to prevent passing parts.
- Trash being removed from a parts location or building must be compacted on site or checked.

Enhanced Security - APC = 2, 3:

Security measures, in addition to Baseline Security:

- Storage and/or work areas where parts are located must be isolated from general access interior building space by using locked enclosure with a controlled access system (CAS).
- Storage and/or work areas must have a controlled access system with individual identification and audit functions. This will include a verification process for all those authorized to enter the area.
- Keys used to access storage and/or work areas must have a management accountability process.
    - Accountability controls for keys in use by multiple people for parts access. Keys must be logged in and out at a central control point.
    - When keys are lost, not returned, or a key is compromised, locks must be changed.
    - Keys must not be used as a normal means of access when a CAS system is employed.
- Break areas should be located outside parts storage or manufacturing areas.
    - Accommodations for personal items should be provided outside of the area.
- Parts or high level assemblies that are too large to easily be removed from the area and not easily dismantled, may remain in a Baseline Security area.

- IBM parts storage will be logistically separate from non-IBM parts and stored in uniquely identified locations when both IBM and other company parts are stored.

Extended Security - APC = 4:

Parts must meet all requirements of Improved Security plus the following requirements. Extended Security storage must be designed and constructed to enhance the protection of parts. Access must be only from interior building space, with no exterior entrances, exits, windows, or skylights.

Sensitive parts must not be left unattended while in manufacturing, assembly, dismantle, repair, test, or labs; and must be maintained in a locked enclosed space when unattended e.g.,. locked carts, tubs, bins, or cabinets. This includes rejected and/or defective parts.

Extended Security consists of a secondary level of limited, controlled access established within the perimeters of the Improved Security requirements of a Parts Storage Facility. Dependent upon local requirements, one of the following methods must be utilized.

Vault (enclosed storage)

An enclosed storage construction with solid walls and ceiling. However, due to variations in types of building material available in different countries, substitutions will be considered as long as equivalent strength and type of material being used is consistent with the requirements. Heavy metal mesh walls are acceptable if the openings in the mesh are small enough to prevent parts from being passed through the structure, and if the walls are strong enough to deter attempts to cut through it. The Asset Protection Functional representative or the APCC representative should be consulted on material substitution, whether the substitution provides equivalent protection.

The following are required for vaults:

- A controlled access system or cipher type electronic lock with individual identification and audit function.
- Astragals (pick plates) as needed for door lock integrity.
- Entrance and exit doors must be alarmed to detect forced entry and to ensure they are secure after use.
- Interior motion detection which is activated during non-business hours or when unoccupied.

Safe or Cabinet

Safe – A “C” rated or TL 15 (or higher) safe is adequate. A “B” rated safe (also known as a “locker”) is also adequate. Safes must be secured to the floor or other fixed building structure.

Cabinet or similar structure - Must be constructed of a solid, heavy duty material that is totally enclosed, with a steel locking bar and Security approved lock. It must be secured to the floor or constructed in such a manner that it cannot be easily removed or has to be fixed to a building structure.

Parts Controls in Development

In a Development Laboratory environment in which parts will be utilized within the Laboratory, and not for external use or consumption, the Asset Protection Functional representative can approve the use of a secured cabinet for APC 4 parts storage, with a controlled access system for the room. The Asset Protection Representative should consult with Security before making this decision. All APC 4 parts must be secured within the Cabinet when not in active use.

APC = 0, 1, 2, 3:

In recognition that classical inventory logistics/parts control systems do not exist in the Development environment, alternative methods for controls may be implemented. It is the responsibility of the Lab Executive to assure that these methods meet the intent of responsible inventory control and loss awareness.

Development must have a management approved and documented process for controlling proprietary parts at suppliers. This must be part of the Product Security Plan and must be reviewed by the unit Asset Protection Functional Area Representative or designee.

APC = 4: Same as above plus-

PN/SN accountability is required as defined.

At times, Development needs to disassemble an FRU kits and/or an assembly in which a previously consumed sensitive part is contained within the assembly. The FRU kit and/or assembly TIN must have a consumption transaction associating the removed sensitive part in CATS. The removed sensitive part will be tracked within development until final disposition.

Unannounced Products

The PDT is responsible for the security of their unannounced products.

Please consult with Global Logistics operations for requirements needed for shipment of unannounced products.

3.2 Inventory Controls

A part will require a specific level of inventory control based on its level of asset protection classification.

Non-Sensitive Parts - APC = 0, 1
PN/Qty Control (Loss Awareness)

- Part number/quantity control throughout the logistical and physical processes.
- Receipt verification process
- Secured containers or tamper evident packaging, that satisfy the Business Unit intent of receipt / shipment accountability.
- Documented management process.

- Any unexplained negative inventory variances out of tolerance after investigation are to be reviewed with Security for the possibility of theft or fraud as documented by the unit's management approved reconciliation process.

Sensitive Parts APC = 2, 3
PN/Qty Control (Loss Awareness/Protected Disposition): Same as APC =0, 1 plus-

- Sensitive parts are to be included in the sample population for cycle and inventory counts.

APC = 4
PN/SN Control - (Loss Accountability): Same as APC = 2, 3 plus-

- Each unit must have a process to verify inventory, by TIN (loss accountability), within an established time period, which should not exceed 90 days. This inventory verification must be recorded in Central Asset Tracking System (CATS) or Local Asset Tracking System (LATS). All quantity and PN/SN discrepancies must be reconciled 100%, with prompt follow up to management.

Lost Part Reporting

Non Sensitive Parts - APC = 0,1;

Follow the locally defined inventory reconciliation and loss reporting process.

Sensitive Parts -

APC = 2; Same as above plus -

When a theft is suspected, it is the responsibility of the Business Unit to report these to security.

APC = 3; Same as above plus -

If the incident is a theft or suspected theft, Security will follow the incident reporting procedures to determine whether the loss will be entered in the Global Incident Reporting System (GIRS). The Business Unit Sensitive Parts Coordinator is responsible for root cause investigation and possible preventative action.

APC 4: Same as above plus -

All unaccounted for parts must be reported as lost (TXN 399) to CATS within 1 business day after the determination is made that the part is in fact unaccounted for or lost.

Note: Legal and regulatory requirements may require that all losses be reported to Security.

4.0 Sensitive Parts Tracking

Tracking is defined as the process of monitoring the movements of APC 4 parts. An APC 4 part will require tracking of the part number and serial number (TIN) through the IBM logistics processes through defined tracking points and provide real-time accountability of the part's movement through point to point recording.

The tracking of APC 4 parts must occur from the point of "creation" or "re-use" to the point of "consumption", "sale" or "final disposition". "Consumption" activities are used to define a part inclusion into a higher assembly, machine, MES or service part replacement.

APC 4 parts consumed in a higher assembly will not be tracked. Tracking will recommence if the consumed part is returned and/or removed from the higher assembly at the first point of an IBM controlled location.

4.1 Self-Audit Requirements

In order to assure APC 4 part tracking integrity, each Macro-Point must conduct a semiannual reconciliation between data in the CATS and the Macro-Point's inventory system. The requirement is that data in the local asset tracking system (LATS), the Central Asset Tracking System (CATS) and the actual inventory must be in sync with each other.

Each Macro-Point must maintain the following through their process documentation:

- Local Self-Audit Process.
- Definition of each self-audit check including timing, sample size, control limits and required actions.
- History of self-audit results. (Current year + 1)
- Reconciliation and follow-ups to include effectiveness/coverage of local processes.

5.0 Protected Disposition

Returned Machines (Section Removed) *Reference Corporate Instruction ISC 163*

5.1 Parts Disposition

- Protected disposition is the assurance that parts are used/reused in accordance with IBM approved processes or impaired/scrapped.
- The objective of protected disposition is to optimize IBM's reutilization potential while maintaining the Asset Protection Initiatives.
- Protected disposition applies to all identified part numbers regardless of their source (new, post-warranty, EC, RPMES/RPEC, dismantle, etc.) or financial ownership.
- All business units handling parts for disposition must have a process to control the return of parts for reuse and have IBM approved reuse processes. If no requirements exist for the part locally, (and if not economical to ship to where there may be requirements) follow the impairment/scrap processes as specified in this document.

5.2 Final Disposition (Impairment / Scrap)

APC = 0

- Implement controls to ensure management approved disposition.
- Adequate security controls are to be in place to protect IBM's interest.
- Impairment methods for media containing IBM or Customer Information must be established with the Unit's Business Controls.
- Authorized scrap supplier will be allowed to dispose of IBM parts reference Section 8.0.
- Approval for disposal or residual recovery suppliers must be obtained from Corporate Environmental Affairs Programs or as delegated to the Unit General Manager.

APC = 1, 2, 3: Same as APC = 0, plus:

Impairment of parts is a process that destroys the function of a part such as to render the value from function negligible and the part unusable and unrepairable. This process allows for the recovery of components for reuse and/or residual materials. Once impairment occurs, the part is no longer considered sensitive.

Impairment Exemptions

- Basic Hardware (brackets, sheetmetal, etc.) does not require impairment.
- Industry standard, Non-IBM Logo'd, Non-FRU parts. i.e. Fasteners, brackets, shafts, hinges, casters, hoses, covers, bezels, etc.
- Cables do not require impairment
- Frame impairment is not required.
- Parts with an electrical hazard concern, such as power supplies & battery back up do not require impairment.

APC 4: Same as APC = 1, 2, 3, plus:

- Parts must be impaired using an approved process defined by the Business Unit and recorded in CATS

6.0 Sensitive Part Sales

This applies to the sale of IBM Sensitive parts to Secondary channels. Secondary channel sale is defined as a non-retail sale to non end users. Business Partners are considered end users. This includes excess/surplus, scrap candidate new and used parts.

GARS is the IBM organization responsible for the placement of IBM's used equipment into the secondary market, including strategy development and right of approval of any/all sales programs introducing used and excess product (including materials/parts). This encompasses the development, coordination, authorization and execution of all secondary channel sales and wholesale broker activity. GARS has responsibility to coordinate with IBM Brands, the ISC and other divisions on an integrated go-to-market strategy for all sales programs of such equipment into the secondary channel.

REF: CP 10.12 - E/S/Z and CI ISC163

Additional Requirements - APC = 3, 4:

- Should not be sold other than to end-using customers through normal marketing channels. Any exceptions must be approved by Global Manufacturing and Integration Supply Chain Manager.
- All sales must be recorded in a central database maintained by GARS.

7.0 Deviations / Escalation

Deviation to CP 10.13

Any request for deviation must be documented with a risk acceptance which complies with Corporate Instruction-Finance 166 and with any specific local requirements.

- Deviations which are permanent in nature and which have adequate secondary controls implemented which effectively mitigate the risk of asset loss do not require a documented risk evaluation when a Key Control over Financial Reporting (KCFR) or a Key Control over Operations (KCO) has been established that independently tests the secondary control(s). The purpose of the KCFR/KCO testing is to validate that the control is working properly. If the control is not mitigating the risk, then additional action is needed to either eliminate the deviation that is creating the risk or to mitigate the risk.

Sensitive Parts Classification Escalation Process

If there are disagreements or issues between Units on the classification of a part, or on data within the part's sensitive part profile, a business case for each unit should be presented through the following representatives until resolved:

1. Sensitive Parts Administrator
2. Asset Protection Peer Council Representatives (consulting with the APCC)
3. Asset Protection Competency Center

8.0 Supplier / Vendor Asset Protection Requirements

Sensitive part numbers are defined by IBM with monetary and/or intellectual value that if lost or stolen would affect IBM negatively. IBM will determine what part numbers are sensitive and assign an asset protection code (APC) value. This information will be available to IBM's suppliers/vendors so they may protect and control these valuable assets to IBM's satisfaction.

8.1 Asset Security

Sensitivity Classification

There are five levels of sensitivity:

APC-0 Non-Sensitive Parts

APC-1 Non-Sensitive Parts with protected disposition controls with baseline physical security.

APC-2 & APC-3 Sensitive Parts that require enhanced physical security.

APC-4 Sensitive Parts that require point to point physical tracking and enhanced physical security.

Physical Security

APC-0 and APC-1 Parts, physical assets and IBM owned machines must be protected in a locked and alarmed enclosed environment, with access limited to management approved personnel. Windows and doors must be locked and any trash being removed must be compacted on site or inspected.

APC-2 and APC-3 In addition to the above for APC-0 and APC-1, storage and/or work areas where parts are located must be isolated from the general access interior building space with controlled access. A documented authorization list and verification process must be in place for all those authorized to enter a parts storage facility. Break areas should not be located inside the parts storage or manufacturing areas.

APC-4 In addition to the above for APC-2 and APC-3, the storage area must be designed and constructed to enhance the protection of parts. Access must be only from interior building space, with no exterior entrances, exits, windows or skylights. The area must have a controlled access system with individual identification and audit function. The area must be alarmed when not occupied.

Note: Parts stored in a Safe or Secured Cabinet met the intent described above.

Safe – A "C" rated or TL 15 (or higher) safe is adequate. A "B" rated safe (also known as a "locker") is also acceptable. Safes must be secured to inhabit removal.

Cabinet or similar structure - must be constructed of a solid, heavy duty material that is totally enclosed with a heavy duty lock. It must be constructed in such a manner that it cannot be easily removed or is fixed to a building structure.

Note: Legal and regulatory requirements may require additional physical security depending on the specific contract.

Inventory Controls

APC = 0, 1, 2, 3:

The supplier will provide inventory verification annually or as defined in the contract.

APC = 4: Same as APC = 0, 1, 2, 3, plus:

The supplier will provide inventory verification quarterly.

8.2 Sensitive Parts Tracking

The following tracking requirements will be required of a supplier who handles APC 4 sensitive parts on behalf of IBM. This will include contracted manufacturing, outsourced activities and repair operations where the supplier handles IBM sensitive parts.

The supplier will be required to provide to IBM the tracking transactions for APC 4 parts as a Macro-Point. Tracking reports from CATS will be provided to the supplier to assist them in meeting the requirements defined in this document.

Tracking provides real-time accountability of parts movement through point to point recording.
The supplier will be required to provide to IBM the tracking transactions for APC 4 parts at their Macro-Point. Tracking reports from CATS (Central Asset Tracking System) will be provided to the supplier to assist them in the control of APC-4 parts.

All unaccounted for APC-4 parts must be reported as lost (TXN 399) to CATS within 1 business day after the determination is made that the part is in fact unaccounted for or lost.

Note: Legal and regulatory requirements may require that all losses be reported to IBM Security.

Each Macro-Point is required to maintain the following roles and responsibilities.

- Macro-Point Management Contact
  - Receives weekly management awareness reports from CATS on tracking activities.
  - Responsible to ensure appropriate actions are being taken by the Administrative Contact
- Macro-Point Administrative Contact
  - Receives daily activity reports from CATS on tracking activities.
  - Responsible for all tracking transactions for the Macro-Point and first point of contact.

Self-Audit Requirements

In order to assure APC 4 part tracking integrity, each Macro-Point must conduct a semiannual reconciliation between data in the CATS and the Macro-Point's inventory system. The key requirement is that data in the local inventory system, the local tracking system, the CATS and the actual physical parts must be accurate and in sync with each other. Each Macro-Point must maintain the following through their process documentation:

- Local Self-Audit Process.

- Definition of each self-audit check including timing, sample size, control limits and required actions.
- History of self-audit results. (Current year + 1)
- Reconciliation and follow-ups to include effectiveness/coverage of local processes. Any necessary transactions must be reported to CATS within one business day of the reconciliation.

Incident Reports

All security related incidents must be reported immediately to the IBM business contact per the supplier contract. These incidents include:

- All incidents of IBM-owned assets.
- Any attempts of theft, fraud, or criminal activity.
- Any event or activity that could impact IBM's business operations, or negatively impact IBM's reputation, through the loss of sensitive parts.

8.3 Protected Disposition

APC = 0, 1, 2, 3:

Impairment of parts is a process that destroys the function of a part such as to render the value from function negligible and the part unusable and unrepairable. This process allows for the recovery of components for reuse and/or residual materials. Once impairment occurs, the part is no longer considered sensitive.

Impairment methods for media containing IBM or Customer Information must be established with the Unit's Business Controls

Supplier scrapping of unimpaired parts is permitted with the following process controls:

- Type(s) of product and characteristics defined
- Identified control points, compliance testing and review plan
- Impairment level and methodology (includes cut, drill and/or shred)
- Storage and physical protection of unimpaired assets

APC 4: Same as APC = 0, 1, 2, 3, plus:

Parts must be impaired by a process approved by the IBM Business Unit. This process must include process controls that include impairment verification and the processing of CATS transactions.

Note: Legal and regulatory requirements may require additional controls depending on the specific contract.

8.4 Supplier Asset Protection Requirements Matrix

Physical Security	**APC 0/1**	**APC 2**	**APC 3**	**APC 4**
Supplier secures parts and IBM owned machines.	standard	enhanced		
IBM can conduct physical security audits at the supplier location.	Dependant on Contractual Agreement			Y
All must have a controlled reclamation and/or scrap process.	Y			Authorized by IBM
Inventory Controls	**APC 0/1**	**APC 2**	**APC 3**	**APC 4**
Root Cause Analysis on all variances	Dependant on Contractual Agreement			Y
Supplier conducts physical inventory and reports results to IBM. Includes reconciliation and detected discrepancies.	Annual			Qtrly
Supplier maintains proper separation of duties in inventory control process	Y	Y	Y	Y
Parts Labeling & Record Keeping	**APC 0/1**	**APC 2**	**APC 3**	**APC 4**
Supplier assures all in-process data collection is traceable to/from the IBM PN/SN (TIN) data	N/A	N/A	Optional	Y
Parts Labeling	PN		PN / SN barcoded	
Shipping & Transportation & Receiving	**APC 0/1**	**APC 2**	**APC 3**	**APC 4**
Packing list to be received by IBM prior to arrival and no more than 48 hours after shipment	N	Y		
Receipt acknowledgment at supplier	PN Qty			PN/SN
Parts are not to be left unattended at supplier dock areas	N	Y		

Appendix A. Asset Protection/Control Matrix for Parts

Control Requirements	0	1	2	3	4
Security (Ref. Section 3.0)					
- Baseline security	**Y**	**Y**	**Y**	**Y**	**Y**
- Enhanced security	N	N	**Y**	**Y**	**Y**
- Extended security	N	N	N	N	**Y**
Control Requirements	**0**	**1**	**2**	**3**	**4**
Inventory Controls (Ref. Section 3.2)					
- Standard inventory controls -Loss Awareness	**Y**	**Y**	**Y**	**Y**	**Y**
- Protected disposition	N	**Y**	**Y**	**Y**	**Y**
- Loss accountability	N	N	N	N	**Y**
Control Requirements	**0**	**1**	**2**	**3**	**4**
Sensitive Part Tracking (Ref. Section 4.0)					
- PN/SN Tracking / Reconciliation	N	N	N	N	**Y**
Control Requirements	**0**	**1**	**2**	**3**	**4**
Labeling (Ref. Section 2.4)					
- Bar code (BC) PN required on part	N	N	**Y**	**Y**	**Y**
- BC PN required on FRU box	**Y**	**Y**	**Y**	**Y**	**Y**
- BC PN/SN required on part	N	N	N	Y	**Y**
- BC PN/SN required on FRU box	N	N	N	N	**Y**
Control Requirements	**0**	**1**	**2**	**3**	**4**
Final Disposition (Ref. Section 5.0)					
- Dismantling of sensitive parts at IBM	Y	Y	Y	Y	**Y**
Control Requirements	**0**	**1**	**2**	**3**	**4**
Supplier Requirements (Ref. Section 8.0)					
- PN/SN Tracking / Reconciliation	N	N	N	N	**Y**
- Inventory controls -Loss Awareness	**Y**	**Y**	**Y**	**Y**	**Y**
- Inventory Controls - Loss accountability	N	N	N	N	**Y**
- Final Disposition	Y	Y	Y	Y	Y

Legend

- Y - Yes, Applicable
- N - Not Required or Applicable

Appendix B. ACRONYMS / DEFINITIONS

APCC	Asset Protection Competency Center
APPC	Asset Protection Peer Council
ARMS	Automated Report Management System
Asset Protection Classification (APC)	Asset Protection Classification. (See Corporate Instruction 10.13 for further definition). A numerical identifier for a part that represents its degree of asset sensitivity.
Baseline Security	Minimal security requirements for parts and/or assets.
BFU	Build From Used (upgrade orders created from used parts)
BP	Business Partner
BPSO	Business Partner Support Operations (Administrative support for Business Partners)
CAS	Controlled Access System
CATS	Central Asset Tracking System
CDA	Confidential Disclosure Agreement
Central RMER Tracking (CRT)	A Lotus Notes Database that allows for individual comments and monitoring of information related to a specific RPMES.
CFO	Customer Fulfillment Organization
CHQ	Corporate Headquarters
Component recovery	The disassembly of a part into select components in order to recover function and/or value from those components.
Consignment Inventory	The underlying substance of consigned inventory is that title continues to reside with IBM. Consignment inventory is the temporary transfer of IBM-owned assets (i.e., raw materials, parts, subassemblies) to a supplier or other party so that they may perform contracted activities or services for IBM. Consignment inventory also includes IBM products shipped to distributors where final sale is contingent upon sale by the distributor and IBM products shipped to subcontract distribution centers.
Consume	An event that terminates the tracking of a specific part at that moment. (The part has become part of another entity, e.g., assembly or machine.)
Controlled Parts	Parts required to be removed from the machine configuration during the installation of a RPMES or RPEC and are itemized for return on the plant enclosed RMER.
CPP/S	Common Parts Process & Systems
Create	The activity which initiates the tracking of a specific new part in a macro-point.
CSO	Customer Support Operations (Administrative support for Sales)
CSP	Certified Service Part(s)
CSR / SSR	Customer Service Rep / System Service Rep
CSU	Customer Set-up (products)
DACS	Distributed Asset Communication System
EC	Engineering Change

EDI	Electronic Data Interchange
Enhanced security	An increased level above Baseline Security of physical security designed to detect and/or deter unauthorized access to parts in storage.
ETN	Equivalent to New
FCSI	Field Change Shipping Instructions
Field Replaceable Unit - Kits (FRU Kits)	A single packed part or assembly, used to replace a defective part in a customer machine. The terms FRU, spare part, service part and field spare are synonymous. A collection of parts within a single FRU part number. This kit may contain a single APC 4 part with other non-sensitive parts. The APC 4 part must be consumed in CATS within the FRU Kit assembly BOM.
Final Disposition	The process by which a part ceases to exist, (e.g., scrap, component recovery).
Finished Goods	A part, assembly or machine that is in a completed manufacturing status.
GA	General Availability
GARS	Global Asset Recovery Services
GIRS	The Global Incident Reporting System (GIRS) allows IBM employees and vendors to submit incident reports involving stolen assets, suspected crimes that have been committed on IBM property or if they were the victim of a crime while representing IBM to IBM Security. Reports are then forwarded to the appropriate security professional for follow-up action.
IBM Employee	A full or part time employee, including a supplemental employee and employees of IBM subsidiaries where IBM owns 51% or greater interest, but not including a vendor, a vendor employee or a subcontractor.
IBM Joint Venture	A corporation or other legal entity that is formed by IBM and others for the purpose of pursuing a specific business objective.
IBM Service Technician (Installer)	An IBM Service Technician (SSR) is a qualified Service Technician authorized to perform the installation of RPMESs or RPECs. This person may either be an IBM employee or a non-IBM Service Technician who is authorized by the General Manager of IBM Global Services and the Director, Global Contracts and Practices.
IBM Subsidiary	A corporation or other legal entity which is more than fifty percent (50%) owned or controlled, directly or indirectly by IBM.
ICI	Installed to Close Indicator
IDDE	International Distribution and Data Exchange
IGF	IBM Global Finance
IGS	IBM Globally Service
Impairment / Scrap	A process that destroys the function of a part such as to render the value from function negligible and the part unusable and unrepairable. At this point, the part is no longer sensitive. This process allows for the recovery of components for reuse and/or residual materials .
Industry-Standard Part	A commercially available generic part with general market availability. It is not IBM unique nor does it or any of its components, have any IBM technology.

Inventory	Any part in a completed and/or functional state. Parts inventory would not include parts that are included in an assembly or a machine awaiting final disposition.
ISC	Integrated Supply Chain
ITS	Integrated Technology Services
KCFR	Key Controls over Financial Reporting
KCO	Key Controls over Operations
LATS	Local Asset Tracking System
LIC	Licensed Internal Code
LICCC	License Internal Code Controlled Configuration
LMT	Lifecycle Management Team
LOEC	Lab of Engineering Control
Loss Accountability	The ability to detect the loss of a single specific part and identify it by part number and serial number.
Loss Awareness	The ability to detect the loss of one or more parts, but not the ability to identify the specific lost part.
M&D	Manufacturing and Development
Macro-Point	Any entity that creates, receives, consumes and/or distributes sensitive parts, and represents either a physical location (site, branch office, etc.) or a defined logistics process within the worldwide IBM Logistics Process. APC 4 parts movements into, out of and between macro-points must be sent to the Central Asset Tracking System.
MD	Microelectronics Division
MES	Miscellaneous Equipment Specifications
Micro-Point	Any entity within the macro-point where activities initiating tracking of parts are processed, and represents either a physical location (warehouse, manufacturing line, dock, etc.) within the defined logistics process or a portion of the defined logistics process.
NBO	New Business Offerings/Opportunity
Non-controlled parts	Parts required to be removed from the machine configuration during the installation of an RPMES that are not itemized for return on the plant enclosed RMER.
Obsolete and Surplus (O&S)	IBM parts in inventory that have been written off financially because either (a) their engineering level no longer meets IBM technical requirements, or (b) inventory quantities exceed present and anticipated needs.
OEM	Original Equipment Manufacturer
Part	Any product, component, assembly or combination thereof, which can be identified by an IBM part number. This include parts, assemblies, options, FRU's, features, bill of materials, etc., irrespective of intended use.
Part Number	The unique alphanumeric identity assigned to reference a particular part.
PDT	Product Development Team

Physical Assets	In reference to CP 10.13 this applies to parts, components, assemblies or any combination thereof that are associated with IBM products. This does not apply to stationery products, furniture, fixtures, tools, etc.
POC	Plant of Control
POM	Plant of Manufacture
PRC	Parts Return Center (Country Parts Return Center)
Projected Installation Date	Applies to a significant delay in installation for valid technical or business reasons.
Proprietary Parts	In contrast to industry-standard parts, proprietary parts are unique to IBM . IBM frequently derives significant revenue and profit from these parts and the finished goods that contain them. Control of proprietary parts at all points of the Integrated Supply Chain, including at suppliers, is necessary to maintain IBM's profitability.
Protected Disposition	The assurance that sensitive parts are used/reused in accordance with the approved IBM processes or impaired/scrapped in accordance to IBM requirements.
RDS	Return Data Set
Re-use Disposition	The process by which a used part is conditioned for a specific reutilization activity .
Receipt	The actual receipt of parts being returned to IBM.
Receipt Point	The physical location where parts are sent for receipt as indicated on the RMER and/or Return Address Label (also known as Parts Return Center).
Reconciliation	Investigating and explaining the discrepancy between an expected return and an actual receipt, including plans for any follow-up steps necessary for final resolution and close-out of the receipt record.
Return	An expected return of parts to IBM as defined by a RMER.
RFA	Request for Announcement
RMAR	Returned Material and Adjustment Report
RMER	Returned Material Equipment Report - document within the RPMES or RPEC shipment that list the controlled parts expected to be returned to IBM
RMER Database (Central)	A Central Database that contains expected return and actual receipt data for all RPMESs and RPECs.
RPEC	Retunred Part Enginerring Change. An engineering change (EC) where at least one removed part is either sensitive or otherwise requires a controlled return to IBM.
RPMES	Returned Parts MES where removed parts are either sensitive or otherwise require a controlled return to IBM. This included both New (RMERTYPE = 4) and Build From Used (RMERTYPE = 9) processes.
RPO	Record Purpose Only MES
RPQ	Request For Price Quotation
RPT	Returned Parts Tracking Module. Allows input of actual RPMES receipt information to be recorded in the RMER DB
S&D	Sales and Distribution

S&U	Shipped and Uninstalled - A shipped MES, RPMES that has neither been cancelled nor installed. (Either cancellation or installation is pending.)
SBS	Side By Side (RPMES Order). A machine upgrade is installed simultaneous with the customers original machine. An RPQ is required to run in parallel for an agreed period of time.
SCI	Shipped to Closed Indicator
Secondary Channels	A non-retail sale to non end users. This includes excess/surplus, scrap candidate new and used parts
Sensitive Part	A part that has significant value to IBM and has an Asset Protection Classification of 2 or 4 (ref. Corporate Procedure 10.13).
Separation of Duties	Separation of duties is an important control. It helps prevent errors or thefts from occurring or going undetected. As a general rule, the same individual should not: - have custody of the asset (e.g., accounts receivable, inventory, bank account) - perform its record keeping - authorize changes to the asset (e.g., credits, shipments, payments) - verify the asset or perform independent checks (e.g., inventory counts, check signing, bank reconciliation)
SII	Shipped to Installed Indicator
SOD	Separation of Duties (matrix)
SPA	Sensitive Parts Administrator
SPD	Sensitive Parts Database
STG	Systems and Technology Group
SUC	Shipped/Uninstalled/Cancelled - A shipped MES, RPMES with a record of cancellation before installation.
Supplier / Outsourced Partner / etc.	A non-IBM entity that has a business relationship with IBM. A company providing industry-standard parts would not meet this definition, unless there was significant risk to IBM's revenue if there was a security problem at the supplier.
SWG	Software Group
Tracking	The process of monitoring (local and central) the movements of a specific part into, out of and between logistics processes by recording its unique Tracking Identification Number (TIN) through defined tracking points (micro/macro).
Tracking Identification Number (TIN)	The unique part identification, composed of the part number and unique serial number, applied to specific asset sensitive parts, to enable them to be tracked.
TSA	Technical Service Letter
TSI	Technical Service Instruction
Unit	Any IBM organization as defined by the business or operation management. An organization with a self contained management structure, which reports to a larger organization structure, which reports to a larger organization or Division.
UOC	Unit of Control
UPR	Used Parts Return

Used Parts	Used parts are parts recovered from returned equipment, field return AFR (Available For Repair) parts, used parts returned via RMER's (Returned Material and Equipment Report) and RMAR's (Returned Material and Adjustment Request).
VPD	Vital Product Data
WAC	Weighted Average Cost