

**Corporate Logistics Procedure 10.13**  
**Asset Protection:**  
**Normal & Sensitive Parts Security**

**Document Number CP10.13**  
**Version 7**  
**04/24/2008**

Document Owner: Integrated Supply Chain  
Asset Protection Competency Center  
Endicott, NY

<b>Preface</b> .....	3
i. Summary of Changes .....	3
ii. Document Change Approvers .....	3
iii. Document Approvals .....	4
iv. Document Review Plans .....	4
v. Document Owner .....	4
vi. Document Distribution/Access .....	4
<b>1.0 Introduction</b> .....	5
1.1 Scope .....	5
1.2 Asset Protection Initiatives .....	5
1.3 Applicability .....	5
1.4 Deviation to CP 10.13 .....	5
<b>2.0 Organization Responsibilities</b> .....	6
2.1 Corporate Operations .....	6
2.2 Asset Protection Peer Council (APPC) .....	6
2.3 Groups / Divisions / Geography's / Organizational Units .....	6
2.4 Security .....	7
<b>3.0 Sensitive Parts</b> .....	8
3.1 Sensitive Parts Definition .....	8
3.2 Sensitive Parts Identification and Process Responsibility .....	8
3.3 Asset Protection Classification (APC) .....	9
3.4 Asset Protection Classification Criteria .....	9
3.5 Sensitive Parts Database (SPD) .....	11
<b>4.0 Asset Protection/Control</b> .....	12
4.1 Security .....	12
4.2 Inventory Controls .....	15
4.3 Sensitive Parts Tracking (APC 4 ) .....	16
4.4 Separation Of Duties .....	18
4.5 Consignment (and Supplier) Relationships .....	18
4.6 Transportation Activities .....	19
4.7 New Machines .....	20
4.8 Returned Machines .....	20
4.9 Protected Disposition .....	21
4.10 Part Sales .....	22
<b>Appendix A. Asset Protection/Control Matrix for Parts</b> .....	23
<b>Appendix D. Corporate References:</b> .....	27
<b>Appendix E. ACRONYMS / DEFINITIONS</b> .....	28
<b>Appendix F. Supplier Asset Protection Requirements Matrix</b> .....	34

# Preface

## i. Summary of Changes

<b>Edition #</b>	<b>Edition Date</b>	<b>Nature of Change</b>	<b>Revision Tag</b>	<b>Date Approved</b>
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		04/24/2008

## ii. Document Change Approvers

The following must review and approve any changes:

- Director, Integrated Supply Chain Operations- WW Manufacturing

This is an approved document. It replaces Corporate Procedure 10.13 issued December 12, 2006

## 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 Corporate 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://w3-9006.ibm.com/isc/distribution/w3wwdams.nsf/C1256B5E00254CB9C12568EA0046AED9/EA9E58B0A67E731E03257337005296F4?OpenDocument>

# 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 and subsidiaries 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. The owner of the supplier process must ensure that all required process controls are in place to protect IBM assets and interests. There are no exceptions to the intent. However, they cannot cover every situation 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 Deviation to CP 10.13

Any request for deviation from CP 10.13 must be documented with a risk acceptance which complies with Corporate Instruction-Finance 166 and with any specific local requirements. In addition, approval of the deviation by the Organization's Asset Protection Executive is required.

- Deviation which are permanent in nature (e.g., parts warehouse where it is not economically feasible to support a vault for APC 4 parts) 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.

## **2.0 Organization Responsibilities**

### **2.1 Corporate Operations**

#### **2.1.1 Asset Protection Competency Center (APCC)**

The APCC is delegated by the Director, Integrated Supply Chain Operations - WW Manufacturing to direct implementation of the asset protection programs /systems. Among its responsibilities are to establish a strategy/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 other divisions and subsidiary headquarters on practices, controls, and other related aspects of the asset protection program.
- Provide advice and guidance through the appropriate headquarters functional units.
- Provide guidance/assistance to the operational units as required.
- Schedule and preside over periodic Asset Protection Peer Council meetings.

#### **2.1.2 Corporate 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 semiannual validation of parts in the SPD.

### **2.2 Asset Protection Peer Council (APPC)**

The Asset Protection Peer Council is 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 of groups, divisions, geography's, and CHQ support organizations.

### **2.3 Groups / Divisions / Geography's / Organizational Units**

Each Unit will identify individuals and develop processes to assure proper implementation / deployment throughout the respective organizations. Each Unit will also define the support structure that will facilitate the implementation of the following activities. 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 Unit will:

- Assign an Asset Protection Executive to be the program leader of the asset protection processes within the Unit. This person is responsible for assuring compliance to this procedure through the levels of the Unit.
- Assign an Asset Protection Peer Council (APPC) Representative to be the conduit for asset protection information between the APPC and the 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.
- Define organizational responsibilities required for the management of the sensitive parts process, including the identification, classification, reclassification, and control.

- 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.
- Communicate to the personnel within the unit, the Asset Protection requirements and educate them regarding their specific responsibilities.
- Establish and identify to the Corporate System Administrator, the Sensitive Parts Administrator (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.

## **2.4 Security**

IBM Security provides advice and counsel for Security programs and practices as well as the investigation of Security incidents. Country or local management will report all thefts and suspected thefts to their respective security functions. Management should consult with 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, minimizing delay and factually representing the events pertaining to the incident. The security function has the responsibility to enter the reported theft or suspected theft, in accordance with corporate reporting guidelines, into the Security Incident Management System (SIMS). 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.

## **3.0 Sensitive Parts**

### **3.1 Sensitive Parts Definition**

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

1. Technology - part has IBM proprietary technology or intellectual property that provides IBM a competitive advantage.
2. 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.
3. Business Unit defined 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

### **3.2 Sensitive Parts Identification and Process Responsibility**

The IBM organization considered as the owner of a part number is referred to in this document as either the Division or Unit of Control (UOC).

The Development Organization releasing a part number has the initial responsibility to evaluate all parts for asset sensitivity in the product development cycle and assign parts protection classifications as appropriate. This sensitive part identification and classification is the responsibility of the Releasing Engineer and the Line Management or assigned representative. Releasing Units are responsible to assure that new products are developed with Asset Protection in mind. Part numbers must be classified before any production starts. This includes engineering prototype (early user hardware) parts.

It is IBM Global Service's (IGS) and IBM Global Finance's (IGF) / Global Asset Recovery Services (GARS) responsibility 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.

It is the responsibility of each Unit of Control to develop a process to identify and classify sensitive parts for its products. 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.

At least twice 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 have not changed. If they have changed, the part and its associated sensitive parts must be reclassified accordingly in the SPD.

In instances where parts are used by multiple Units, the user with the highest APC Classification needs to determine the asset sensitivity for the part. In the case where this user is not the Unit of Control, the user must document its need and justification to the Unit of Control. The Unit of Control, upon acceptance of this request, establishes and/or maintains the part's sensitive part profile. The Unit of Control may also transfer ownership.

Each Unit of Control will determine and document its criteria for classifying a part as sensitive, as well as the level of classification, 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

Asset sensitivity decisions are made at the part number level, for each part. 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 however 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. The classification process should take into account the sensitivity of an assembly and/or its parts in applications other than its intended function.

### **3.2.1 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 Executives
4. Manager of Asset Protection Competency Center
5. Director, Integrated Supply Chain Operations- WW Manufacturing

### **3.3 Asset Protection Classification (APC)**

The Asset Protection Classification is a numerical identifier that represents the degree of sensitivity. The Asset Protection Classification also determines the control requirements for asset protection. Every IBM part number not contained within the Sensitive Parts Database will be assigned an Asset Protection Classification 0. Any part with an APC value of 1 is not considered sensitive, but has a protected disposition. Any part assigned an APC of 2, 3, or 4 is considered sensitive. All parts with APC classification 1-4 must be entered in the Sensitive Parts Database (SPD).

### **3.4 Asset Protection Classification Criteria**

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

#### **APC = 0:**

Any part that doesn't meet the Asset Protection criteria listed below for APC 1, 2, 3, or 4 and is not asset sensitive. The parts require basic inventory and disposition control.

#### **APC = 1:**

A part that has reutilization value and as such requires a protected disposition. APC 1 parts are not considered a sensitive part, but do require disposition controls

**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: (Not Used with current requirements)**

A part that has high risk of warranty fraud.

General guidelines are:

- A part that has increased risk for theft or fraud.
- A part that requires serial number identification.
- This classification can be used when warranty fraud issues are a concern.

**APC = 4:**

A part that has significant value to IBM, and as such requires TIN accountability via point to point tracking. A part that is a critical component of a product upgrade path. Loss or misappropriation of parts in this category would have significant impact on business unit revenue.

General guidelines are:

- A member of the set of highest value parts of a product that contain a significant proportion of its market value.
- A part that has technical sensitivity after GA.
- A part that has high risk for theft or fraud.
- A part with high market value because there is a large market demand relative to general supply.
- Liability to Legal and Regulatory requirements

**Note:**

- 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.
- Machines that are purchased as an IBM part number, usually for inclusion in another product, must be assessed for appropriate APC classification and the classification applied to the PN in the SPD.
- The APC 4 part contained within kits must be consumed in CATS .
- APC 9 is a valid code that may be used by Service NBO to track Non-IBM parts based on Service requirements.

### **3.5 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. This must be completed by the Unit SPA.

The SPD is corporate-wide and is available to all units who handle IBM parts to enable them to implement the required controls (as applicable) for 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 valid DOU with the APCC, including any strategic suppliers with proper agreements in place to receive this information. The SPD is limited to those with a "need to know".

The APC Value in Product Manager reflects the APC code at the time of part release, where applicable to each Unit of Control. This APC Value in Product Manager does not have to be updated upon subsequent reclassification of the part.

## 4.0 Asset Protection/Control

### 4.1 Security

Refer to IBM Security Manual ( PS00, PS01, PS02, PS11) for further details on physical security requirements. Below are the minimal requirements for physically securing sensitive parts, machines and physical assets. Based on organizational results, additional requirement may be required.

#### 4.1.1 Parts, Machines and Physical Assets

##### APC = 0, 1:

##### Fundamental security

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

- Minimize entry and egress points.
- Perimeter doors designated as entrances or emergency exits must be constructed of heavy duty material with a locking device. (Refer to IBM Security Requirements Manual, “Building Perimeters and Interior Security (PS02)”.)
- Windows on the ground floor where parts are stored must be:
  - Inoperable and/or locked.
  - Screen in such a manner to prevent parts to pass thru
- Exterior glass doors and windows in unattended parts storage areas must be covered to prevent the creation of an attractive theft target.
- Trash being removed from a parts location or building must be compacted on site or checked by one of the following methods:
  - Visual Inspection
  - Metal Detection
  - X-ray Device

Consult with local security organizations for advice and counsel on local implementation requirements.

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

##### Improved security

Security measures, in addition to Fundamental security:

- Storage and/or work areas where parts are located must be isolated from general access interior building space by using locked enclosed and alarmed storage with controlled access.
- A controlled access system with individual identification and audit functions.
- A documented authorization list and verification process must be in place for all those authorized to enter a parts storage facility. Refer SECMAN PS05.
- Keys used to access parts 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.
- Windows on the ground floor where parts are stored must be:
  - Alarmed to detect unauthorized entry (e.g., motion detection, glass breakage, etc.).
  - Covered (e.g., shades, blinds, curtains, etc.) to restrict view from the exterior of the building.
- Break areas should not be located inside parts storage or manufacturing areas.
- Accommodations for personal items should be provided outside of manufacturing locations and multi-person access storage areas.

## **Manufacturing and Remanufacturing Locations**

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.

## **High Volume Parts Storage (Warehouses)**

In a warehouse environment, in addition to the Improved security requirements listed above, the following items must be included:

- If the parts storage area is not separated from the administration area, a controlled access system or cipher type electronic lock with audit capability must be used to access the storage warehouse area. Sensitive parts storage must be physically separated from the general building access areas (i.e., public space such as lobbies) by a fence, heavy gauge wire screening or sheathing designed to prevent parts from being passed over or through the structure or wall.
- 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.
- Parts shipments in bulk, palletized shrink wrapped and/or banded with tamper evident seals, received as shipped (with original packaging and sealing intact), may be stored by systematic logistic placement. A documented process for loss detection, reporting, and reimbursement must be in place.

## **Incident Reports:**

All security related incidents within IBM facilities must be reported immediately to IBM Security. At supplier facilities, these incidents must be reported immediately to the IBM business contact for the supplier contract. These incidents include:

- All incidents or suspected incidents of IBM asset thefts.
- 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.

**Note:** The "Terms and Conditions" section of contracts for IBM parts, machines and physical assets located at supplier locations and distribution centers must contain the above requirements.

## **APC = 4: Same as APC = 2, 3 plus:**

### **Extended security**

Parts requiring Extended Security must meet all requirements of Improved security plus the following requirements.

**Note:** IBM Local Security should be contacted for guidance in establishing security controls.

## **Manufacturing, Remanufacturing and Parts Storage Locations**

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.

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. IBM Security 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.
- Panic alarm(s) continuously monitored at a staffed security, control center or central monitoring station.
- Interior motion detection which is activated during non-business hours or when unoccupied.
- CCTV recorded at a staffed security control center or central monitoring station. It is recommended that the CCTV be "event driven" (e.g., triggered by motion detection), otherwise it should be continuously recording. For advice, contact IBM Local Security.

### **Safe or Cabinet**

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

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

### **Engineering Development and Test**

In a Development Laboratory environment in which parts will be utilized within the Laboratory, and not for external use or consumption, the Asset Protection Executive can approve the use of a secured cabinet for APC 4 parts storage, with a controlled access system for the room and without the use of interior motion detection, and without CCTV. The Asset Protection Representative should consult with IBM Security before making this decision. All APC 4 parts must be secured within the Cabinet when not in active use.

APC 4 parts that are intended to be installed into models or prototype appliances for use outside of the lab must adhere to all of the requirements defined within. That is, if the development unit is fulfilling the role of early-manufacturing by building prototypes or models to be sent to other companies (e.g., joint development alliances, business partners, application enablers, etc.) or to be sent to other locations, then all of the requirements apply, as they would to a standard manufacturing operation.

#### **4.1.2 Unannounced Products**

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

### 4.1.3 Special Consideration Environment, Global Services and Sales & Distribution

Service technical management must take reasonable measures to protect parts and/or physical assets entrusted to technicians in the scope of their responsibility.

**Note:** Appendix: Special Considerations Environment.

## 4.2 Inventory Controls

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

### **APC = 0, 1 PN/Qty Control (Loss Awareness)**

- The basic principle in parts control is that inputs and outputs must balance on a part number/quantity basis as parts move through the various logistics and business processes, both within and across unit boundaries.
- Establish verification upon receipt (i.e., counting every piece, weigh or count selected items, acceptance of certified supplier counts). Scale counts are accepted under local controls.
- Secured containers or tamper evident packaging, that satisfy the intent of precise accountability or shipment accountability (in the case of scrap) are an acceptable alternative.
- Documented management processes must exist to assure management awareness of parts control posture in the organization.
- Control is maintained through process documentation, precise counts, records and reconciliation to the required levels, detection of loss and correction of any out of tolerance conditions that may exist and appropriate reporting to Security, line and financial management where variances exist above approved levels in accordance with Corporate Financial guidelines. (Ref. AP19 - Inventory Verification / IBM005)
- Counts must include parts in used parts inventory with the same part number.
- Any unexplained negative inventory variances out of tolerance after investigation are to be reviewed with local security organization for the possibility of theft or fraud as documented by the unit's management approved reconciliation process.

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

- PN/Qty accountability must be maintained.
- 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 Cental 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.

### **4.2.1 Parts Controls in Development**

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

**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. The methods and systems implemented must be approved by the Unit Asset Protection Executive and the Business Unit Controller.

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 Executive or designee.

**APC = 4: Same as above plus-**

PN/SN accountability is required as defined.

At times, Development needs to disassemble 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.

**4.2.2 Lost Sensitive Part Reporting and Investigation****APC = 0,1;**

Do not need to be reported in Loss Incident Database.

**APC = 2,3; Same as above plus -**

Losses or suspected losses where theft is suspected, will be reported by the unit into their local Security Incident Reporting System (SIRS) or equivalent reporting system to record the details of the incident.. Each business unit must have a loss reporting process that includes establishing the time frame for recording suspected thefts.

**APC 4: Same as above plus -**

If the incident is a theft or suspected theft the incident is recorded by Security in the Security Incident Management System (SIMS). The APCC will record the theft incident in the Loss Incident Database and assign the incident to the responsible Asset Protection Peer Council representative for root cause investigation and possible preventative action.

All non-theft losses of APC 4, it is responsibility of the Units Asset Protection Peer Council member or supporting staff for entering unaccounted/unexplained loss into the Loss Incident Tracking Database.

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

**4.3 Sensitive Parts Tracking (APC 4 )**

Tracking is defined as 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 point. Tracking provides real-time accountability of parts movement through point to point recording of this movement.

- The unit must also define the tracking points (Macro-Points) where tracking data will be recorded and sent to the Central Asset Tracking System (CATS).

- Each unit must develop the process and/or systems to perform the tracking activities.
- All Macro-Point transactions must be recorded within 1 business day of the tracking event (occurrence of the activity) 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 and effectiveness per the requirements of this procedure.
- Each Unit must define and implement a tracking practice for APC 4 parts handled by a supplier. This may be either at the macro- or micro-point level with consideration to the other requirements of CP 10.13.

An APC 4 part will require tracking of the part number and serial number (TIN) through the IBM logistics processes. This tracking is applicable to all APC 4 parts regardless of their status including, but not limited to: new and used manufacturing and service parts, warranty and post warranty parts, including defective parts, prototype parts, engineering parts and reuse parts.

The tracking of these parts must occur from the point of "creation" or "re-use" to the point of "consumption", "sale" or "final disposition" (impairment or scrap.) "Consumption" activities include but are not limited to the inclusion in higher assembly, machine, MES or service part replacement.

**Note:** Once consumed, a part will no longer be tracked. APC 4 parts consumed in a higher assembly will not be tracked. Tracking will recommence if the consumed part is returned and/or removed at the first point of IBM controlled location. If the assembly itself is also an APC 4 the assembly must be tracked. Parts must also be tracked through all transfer activities between Macro-points.

#### **4.3.1 Self-Audit Requirements**

In order to assure tracking integrity, each Macro-Point must conduct semiannual correlation 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 synch 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.

#### **4.3.2 Asset Tracking Responsibilities**

##### **4.3.2.1 Corporate Operations (System Owner)**

Corporate Operations serves as the Asset Tracking Process / System Owner and maintains the responsibilities for defining the asset tracking process and systems requirements. It is also the owner and administrator of the Central Asset Tracking System and is responsible for operational, maintenance and development activities. These responsibilities are delegated to the Asset Protection Competency Center.

##### **4.3.2.2 Macro-Point Responsibilities**

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

- Macro-Point Management Contact
- Macro-Point Administrative Contact

### 4.3.3 Part Identification Labeling Requirements

- All sensitive parts must be properly labeled prior to movement, irrespective of where the part is, as either individual parts or in assemblies or machines.

**Note:** For parts returned from Service the requirement for package labeling will be defined by the receiving and sending Units.

**Note:** 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 Guides, CS 0-5103-007.

#### 4.3.3.1 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 # and TIN number (in 11S format) must be on the outside of the package, as well as the human readable FRU #. The FRU TIN labeling on the box must be identical to the FRU 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 to the TIN label.

#### 4.3.3.2 APC = 4:

It is the responsibility of each unit handling non-labeled parts to ensure that trackable asset sensitive parts are labeled via 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 and see Global Label Guide (31L5241) and CS-0-5103-007 for details.

### 4.4 Separation Of Duties

**Note:** Ref. Corporate Instruction FIN 183

### 4.5 Consignment (and Supplier) Relationships

(Ref. Appendix: Supplier Requirements Matrix)

#### APC = 0, 1, 2, 3:

- IBM Procurement handles or assigns all contacts and contracts with suppliers.
- All consigned scrap, overruns, etc., will be disposed per the requirements defined in Section 4.9 Protected Disposition.
- Suppliers acknowledge receipt of consignment in timely fashion.
- Suppliers must notify IBM immediately upon actual loss or 3rd party attempt to get parts. IBM contact will notify the appropriate local organizations, (security, consignment inventory control) of such occurrences.
- Accountability for consigned parts will be assured by consigning location; controls of inventory, returns, scrap, salvage, reconciliation of discrepancies and follow-up, variance trending and similar controls will be assured.

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

- If consignment is necessary, for M&D sites the Product Manager and the unit Sr. Procurement Manager must approve the consignment relationship with the supplier. For other business units the unit's Asset Protection Executive must approve the business relationship.
- Supplier must not consign to a 3rd party without the unit's Sr. Procurement Manager's or Asset Protection Executive's written (or electronic) permission.
- Sale of parts as an alternative to consignment, may be made only on an exception basis and then with the prior approval of the unit's Sr. Procurement Manager, site Controller and site General Manager for M&D sites, only for use in product/assembly being manufactured by supplier for use by IBM. For other business units the unit's Asset Protection Executive must grant approval.
- Parts shall not be marked with the supplier's name or logo unless required for regulatory compliance.
- With the supplier, IBM will inventory the consigned material at least QUARTERLY. (If the quantity of parts consigned to a supplier is low, supplier counts may be accepted with approval from local line and financial management).

#### **4.5.1 Supplier Tracking Requirements**

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

Procurement Peer Council representative will be the first point of escalation on any issues related to Supplier Tracking Requirements.

Refer to Appendix: Supplier Asset Protection Requirements Matrix for details.

#### **Physical Security**

The supplier will conform to the requirements defined.

#### **Tracking Requirements**

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.

#### **4.6 Transportation Activities**

Any loss, damage or tampering of a shipment must be reported to the Global Logistics' contact in accordance to local requirements and guidelines.

Ref. Appendix: Supplier Asset Protection Requirements Matrix

Ref. C-B 0-3700-000, "Tamper Evident Sealing of IBM Assets"

Tamper Evident Seals must be protected as defined in C-B 0-3700-000.

#### **APC = 0, 1:**

- Global Logistics is responsible to provide/implement appropriate transportation and storage processes, as specified in the Global Logistics Guidelines.
- Sealed boxes / Strapped pallets or similar tamper evident detection is required.

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

- Visible packaging/documentation must not identify shipment as containing sensitive parts.
- Tamper Evident Seals or Tape are required

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

- Ship notification/receipt acknowledgment by sending the appropriate tracking transactions to CATS.

## **4.7 New Machines**

*Section Removed*

## **4.8 Returned Machines**

This section applies to IBM (owned) logo machines or non-logo machines for which IBM owns, or has taken ownership. The intent is to identify and protect IBM machines being returned to IBM or under IBM's control. Each unit is responsible for developing a return process consistent with probable parts content as determined and communicated to them by the SPD or the Unit of Control, if actual content is not available. Protection within the return process is applicable at the first point of IBM control of the asset.

For non-IBM logo machines that become IBM property, e.g., trade-in, or for disposal of machines per customer request, processes must exist to ensure secure storage until disposition.

Each organization must ensure that processes are in place to identify and control the return or disposition of machines canceled after shipment.

All units with disposition requirements for returned equipment, working jointly with Global Asset Recovery Services (GARS) must develop a process to ensure opportunities for re-use are explored before final disposition of the machine. If reuse at the machine level is not practical, machines are to be dismantled at an IBM or IBM-contracted and approved reutilization location. Controls must be in place to ensure recovery of parts with known re-use requirements. For requirements for recovered parts for re-use or final disposition refer to the applicable sections in this document.

The return location must ensure the security of the returned machine until re-use or final disposition of the machine. This includes control of both the machines and the parts in them. Documentation must be maintained of machine movement and any part removal.

### **4.8.1 Take Back Programs**

This section applies to machines that become property or are consigned to IBM through a Take Back or customer-initiated disposal program.

#### **IBM Logo**

The unit handling these machines must ensure appropriate controls and secure storage until disposition. Once in a parts-recovery process, the requirements of CP 10.13 apply to IBM parts only.

#### **Non-IBM Logo**

The unit handling these machines must ensure appropriate controls and secure storage until disposition.

## **4.9 Protected Disposition**

### **4.9.1 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, RPFES/RPEC, dismantle, etc.) or financial ownership.
- All units handling parts for disposition must have a process to control the return of parts for reuse, have IBM approved reuse processes for parts with reuse requirements, and if no requirements exist for the part locally, (and if uneconomical to ship to where there may be requirements) follow controlled impairment/scrap processes as specified in this document.

#### **4.9.2 Final Disposition (Component Recovery, Impairment/Scrap)**

##### **APC = 0**

- Implement controls to ensure management approved disposition.
- Prior to impairment/scrap, a determination needs to be made concerning the recovery of any reusable components on the part. Any non-sensitive components recovered are subject to gross inventory controls until placed in a used parts inventory system.
- Authorized scrap supplier will be allowed to dispose of IBM parts with compliance testing defined by the process owner.
- Once part identification is lost to a P/N level, controls are to be maintained at a weight level, or equivalent, for items where residual recovery is expected.
- Approval for disposal or residual recovery suppliers must be obtained from Corporate Environmental Programs or as delegated to the Unit General Manager.
- 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.

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

Supplier scrapping of unimpaired parts is permitted with each unit's Business Controls and Asset Protection Representative approval, with process controls and compliance testing.

Once impairment occurs, the part is no longer considered sensitive. The process controls must include the following criteria:

- Type(s) of product and characteristics
- Identified control points, compliance testing and review plan
- Separation of duties matrix
- Reconciliation of inputs vs. Outputs (cases or weights)
- Impairment level and methodology
- Storage and physical protection of unimpaired assets

##### **APC 4: Same as APC 1, 2, 3 plus:**

- Parts must be impaired by IBM or by an approved supplier under 100% IBM control.
- APC 4 parts, that are the property of a supplier, shall be disposed of as if it was the property of IBM. IBM may permit, on a documented case-by-case basis, limited final disposition by the supplier to support failure analysis, destructive testing, warranty claims with the supplier, and etc.

#### **4.10 Part Sales**

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

#### **4.10.1 Secondary Channel Sales Responsibilities:**

REF: CP 10.12 - E/S/Z and CI T&M163

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.

#### **APC = 0, 1, 2, 3 :**

The following process must be performed prior to the selling of any IBM parts

- Internal IBM advertisement of E/S/Z parts per CP 10.12.
- All sales must be recorded in a central database maintained by GARS. Information for all sales must include; Date, Part Name and Description, Part Number, Quantity Sold, WAC, Sale Price, Sales location, Broker Name and Address.

#### **APC=4: All the above, plus:**

- APC 4 will not be sold other than to end-using customers through normal marketing channels. Any exceptions must be approved by Director, Integrated Supply Chain Operations- WW Manufacturing and documented.

## Appendix A. Asset Protection/Control Matrix for Parts

**Note:** This table applies to parts owned by IBM and proprietary parts where there is supplier risk as covered under 'Supplier' in Definitions.

### Legend

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

Control Requirements	0	1	2	3	4
<b>Security</b> (Ref. Section 4.0)					
- Fundamental security	Y	Y	Y	Y	Y
- Improved security	N	N	Y	Y	Y
- Extended security	N	N	N	N	Y
<b>Inventory Controls</b> (Ref. Section 4.2)					
- Standard inventory controls -Loss Awareness	Y	Y	Y	Y	Y
- Protected disposition	N	Y	Y	Y	Y
- Loss accountability	N	N	N	N	Y
<b>Sensitive Part Tracking</b> (Ref. Section 4.3)					
- PN/SN Tracking / Reconciliation	N	N	N	N	Y
<b>Labeling</b> (Ref. Section 4.3.3)					
- 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	N	Y
- BC PN/SN required on FRU box	N	N	N	N	Y
<b>Shipping/Transport Activities</b> (Ref. Section 4.6)					
- Ship-Receipt reconciliation	Y	Y	Y	Y	Y
- Ship-Receipt notification	N	N	N	N	Y
- Tamper Evident Packaging/Sealing	N	N	Y	Y	Y
<b>Final Disposition</b> (Ref. Section 4.9.2)					
<b>Component Recovery</b>					
- Dismantling of sensitive parts at IBM	N	N	N	N	Y
- Impairment by IBM	N	N	N	N	Y
<b>Supplier scrap</b>					
- Dismantling of sensitive parts by IBM	N	N	N	N	Y
- Impairment by IBM or designated supplier with IBM witness	N	N	N	N	Y
- Dismantling by supplier under IBM control	Y	Y	Y	Y	Y
- Impairment by supplier (under IBM control)	Y	Y	Y	Y	N

## **Appendix B. Special Consideration Environment (Ref. Section 4.1.3)**

Any exceptions to this process must have the Geography Director of Security's written approval, including customer locations that may appear to have improved security other than described below.

### **PHYSICAL SECURITY FOR LOCATIONS WITH LESS THAN \$250,000 USD SELL PRICE (for 3 Consecutive Months)**

Sell Price is defined as the total volume of Sensitive Parts at a defined monthly frequency multiplied by the Over the Counter Price. Each Asset Protection Peer Council Representative must approve the business unit process using this security level.

- Must maintain parts in a locked enclosed storage environment, which is a structure surrounding a storage space on all sides, including the top and bottom for the protection and control of access to parts and/or physical assets. Structure material must be such the parts cannot be passed outside of the enclosure.
- For customer only locations, non-APC4 parts which do not fit in the cabinet should be otherwise protected through physical or inventory controls. Controlled access computer room storage is acceptable if removal of parts is limited to authorized personnel.
- Minimize entry and egress points.
- Parts storage locations should be physically separated from the parts drop points to prevent courier access to inventory.
- Perimeter doors designated as entrances or emergency exits must be constructed of heavy duty material with a locking device.
- Each entrance door must be monitored to ensure that it is secure after use.
- If Emergency exit-only doors are utilized, they must have alarms.
- Windows on the ground floor where parts are stored must be inoperable and/or locked. Operable windows on the ground floor must be constructed or adapted to avoid undetected/unauthorized access. Parts should not be visible from any window/door from outside the space. If exterior windows are present, window coverings (e.g. glazing) should be in use to restrict view from the exterior of the building.
- Trash being removed from a parts location or building must be compacted on site or checked by one of the following methods: Visual inspection, Metal detection or X-ray device.
- All APC4 (TIN) parts are stored in a secondary locked environment.
- Non-APC4 bulk parts which do not fit in the cabinet should be otherwise protected through physical inventory controls.
- If keys are in use, a process must be in place to account for all keys issued for parts storage areas. These controls should extend to parts storage cabinets with key locks. Key logs should be maintained with a documented quarterly review to verify key distribution.
- Customer controlled access to parts storage areas must be reviewed quarterly to ensure only authorized access is maintained.
- A process must be in place to control access to the inventory location. Combinations should be changed no less than yearly and sooner based on management discretion when an employee has been separated or if there is suspected or actual compromise.
- Although, the use of personally owned vehicle (POV) is strongly discouraged for parts storage, it is acknowledged that instances of this nature may be required. If so, the following must be adhered to:
  - Assets must not be visible from outside the vehicle.
  - Vehicle must be locked when not in use.
  - Vehicle must be parked in a safe location when not in use.
  - Assets must be removed from vehicle and secured when the vehicle is used for non-business or has to be maintained by someone other than the employee.

- APC 4 parts are not eligible for stocking in a POV inventory location.
- Inventory should be kept to a minimum.

**PHYSICAL SECURITY FOR LOCATIONS WITH MORE THAN \$250,000 USD, BUT LESS THAN \$2,000,000 USD SELL PRICE (for 3 Consecutive Months)**

In addition to the controls outlined above, the following applies:

- Customer Premise
  - Parts are to be maintained in a locked enclosed storage, i.e. cabinet with a steel locking bar and combination lock approved by IBM Security.
  - Large parts are to be maintained in a locked, solid wall and ceiling enclosed storage, i.e. room with motion detection activated when unoccupied.
- Off Customer Premise - IBM and/or Shared Supplier IBM/Non-IBM Outside Location
  - Cipher combination lock with combinations changed quarterly or controlled access system for perimeter door access.
    - Note: Locations in this category established after 05/01/2006 require cipher locks that have individual identification and audit functions.
  - Combinations MUST be changed on these locations whenever anyone is separated from the business.
  - Motion detection alarm, activated when unoccupied.
  - Sensitive parts (APC4 - TIN) parts requiring extended security, must be in an additional locked enclosed storage, i.e. Enclosed heavy duty chain link fence, locked cabinet and a steel locking bar with an IBM Security approved lock or a safe. Access must be limited to authorized personnel with an audit trail of access maintained.

## Appendix C. Impairment Exemptions

1. Exemptions to IBM witnessing of APC - 0,1,2,3 parts:

Supplier scrapping of unimpaired parts is permitted with each units Business Controls and Asset Protection approved process controls and compliance testing. Reference section 4.9.2 Final Disposition

2. Basic Hardware does not require impairment.

- Industry standard, Non-IBM Logo'd, Non-FRU parts.
- i.e. Fasteners, brackets, shafts, hinges, casters, hoses, covers, bezels, etc.

3. Cables

- Cables do not require impairment.

4. Frame impairment

- Frame impairment is not required.

5. Electrical Hazard

- Parts with an electrical hazard concern, such as power supplies & battery back up do not require impairment

6. Impairment Guidelines

Reference Impairment Guideline on the GARS Operations Web site for additional impairment guidelines (

<http://gars.endicott.ibm.com/gars/arsdoc.nsf/MasterDoclibFrameset?OpenFrameSet&Frame=NotesView&Src=/gars/arsdoc.nsf>)

## **Appendix D. Corporate References:**

Corporate Accounting Instruction IBM00-005 Rotating Inventory Audits of Inventories Conducted by Finance

Corporate Accounting Practice 20 - Consignment Inventory Accounting and Control

Corporate Bulletin - C B 0-3700-000, Tamper Evident Packaging

Corporate Instruction

- CCR 105- Donation of Equipment
- ENV 109 - Environmental Evaluation of Suppliers: General and Production Procurement, Waste and Product Disposal
- ENV 116 - Environmental Impact Assessments (EIA)
- ENV 117 - Product Environmental Profiles
- FIN 116 - Sale of Consignment of Parts
- FIN 166 - Risk Acceptance
- FIN 183 - Separation of Duties
- LER 104 - IBM Business Operations Under The International Traffic In Arms Regulations (ITAR)
- IPL 106- Receipt and Disclosure of Confidential Information
- LEG116: Classification and Control of IBM Information
- T&M 144 - Service Parts Lifecycle Management
- T&M 163 - Global Asset Recovery Services

IBM99-005 Accounting for Plant on Loan (JMET)

Corporate Policy Letter # 139 - Environmental Affairs

Corporate Procedure 10.12 - Surplus, Excess, Scrapable Inventory

Corporate Procedure 10.15 - Asset Protection: Returned Parts MES and EC Process Requirements

Corporate Procedure 10.17 - Precious Metals

Global Logistics Guidelines

Global Labeling Guidelines

- Corporate Standard - C-S 1-1121-015, Automatic Identification

Corporate Standard - C-S 0-2535-004, Serial Numbering of Printed Circuit Panels, Cards and Boards

Corporate Standard - C-S 0-5103-007, Reutilization of Parts in IBM Products

GA21-9261 - IBM General Packaging Spec

IBM Integrated Product Development (IPD) Process

US Export Regulation Procedures, USERP (Crypto document)

## **Appendix E. ACRONYMS / DEFINITIONS**

### **ACRONYMS**

AI	Automatic Identification (Bar Code)
APC	Asset Protection Classification
APCC	Asset Protection Competency Center
APPC	Asset Protection Peer Council
ARMS	Automated Report Management System
CATS	Central Asset Tracking System
CD	Compact Disc
CDA	Confidential Disclosure Agreement
CHQ	Corporate Headquarters
CPP/S	Common Parts Process & Systems
CSP	Certified Service Part(s)
DACS	Distributed Asset Communication Service
DIMM	Dual Inline Memory Modules
DVD	Digital Versatile Disc
EDI	Electronic Data Interchange
ETN	Equivalent to New
FRU	Field Replaceable Unit
FSI	Financial Services International
GA	General Availability
GARS	Global Asset Recovery Services
GPS	Global Parts System
IDDE	International Distribution and Data Exchange
IGF	IBM Global Finance
IGS	IBM Globally Service
IMD	IBM Microelectronics Division
ISC	Integrated Supply Chain

ITS	Integrated Technology Services
LIC	Licensed Internal Code
LICCC	License Internal Code Controlled Configuration
LMT	Lifecycle Management Team
LOEC	Lab of Engineering Control
M&D	Manufacturing and Development
MCM	Memory Control Module
MES	Miscellaneous Equipment Specification
NBO	New Business Opportunity
O&S	Obsolete and Surplus
OEM	Original Equipment Manufacturer
PCMCIA	Personal Computer Memory Card International Association
PDT	Product Development Team
PIE	Parts Information Exchange
POC	Plant of Control
POM	Plant of Manufacture
RFA	Request for Announcement
RDS	Return Data Set
RPEC	Returned Part EC
RPMES	Returned Part MES
S&D	Sales and Distribution
TSI	Technical Service Instruction
SIMM	Single In-line Memory Module
SIMS	Security Incident Management System
SOD	Separation of Duties (matrix)
SPA	Sensitive Parts Administrator
SPD	Sensitive Parts Database
STARS	Loss and Damage Tracking system
SWG	Software Group

TSA	Technical Service Letter
TIN	Tracking Identification Number
UOC	Unit of Control
UPR	Used Parts Return
VPD	Vital Product Data
WAC	Weighted Average Cost

## Definitions

Asset Protection Classification (APC)	A numerical identifier for a part that represents its degree of asset sensitivity.
Component recovery	The disassembly of a part into select components in order to recover function and/or value from those components.
Consignment Inventory	(Definition from Corp. Accounting Practice #20..... dated 3/27/97) 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.)
Create	The activity which initiates the tracking of a specific new part in a macro-point.
Field Replaceable Unit (FRU)	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.
Field Replaceable Unit - Kits (FRU Kits)	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.
Fundamental Security	Minimal security requirements for parts and/or assets.

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.
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 Subsidiary	A corporation or other legal entity which is more than fifty percent (50%) owned or controlled, directly or indirectly by IBM.
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 (e.g., plastics, metals, etc.,).
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.
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.
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.
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.
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.
Operational Unit	An organization with a self contained management structure,

	which reports to a larger organization structure, which reports to a larger organization or Division.
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.
Extended security	An increased level above Improved Security of physical security designed to detect and/or deter unauthorized access to parts in storage.
Improved security	An additional level of physical security above fundamental security for parts/assets in storage.
Part Number	The unique alphanumeric identity assigned to reference a particular part.
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.
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.
Re-use Disposition	The process by which a used part is conditioned for a specific reutilization activity (e.g., ETN, CSP).
Secondary Channels	A non-retail sale to non end users. This includes excess/surplus, scrap candidate new and used parts
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: <ul style="list-style-type: none"> <li>• have custody of the asset (e.g., accounts receivable, inventory, bank account)</li> <li>• perform its record keeping</li> <li>• authorize changes to the asset (e.g., credits, shipments, payments)</li> <li>• verify the asset or perform independent checks (e.g., inventory counts, check signing, bank reconciliation)</li> </ul>

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.
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.
Unit	Any IBM organization as defined by the business or operation management.
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).

## Appendix F. Supplier Asset Protection Requirements Matrix

**Note:** This table applies to parts owned by IBM and proprietary parts where there is supplier risk as covered under 'Supplier' in Definitions.

<b>Labeling &amp; Record Keeping</b> (Ref Section 4.3)	<b>APC 0/1</b>	<b>APC 2/3</b>	<b>APC 4</b>
Supplier assures all in-process data collection is traceable to/from the IBM PN/SN (TIN) data	N/A	N/A	Y
Changed PN/SNs to be communicated to IBM within 2 business days.	N/A	N/A	Y
IBM will identify the format & content for all S/N's	N/A	N/A	Y
Shipping, Receiving, Audits, Variance, S/N tracking retention time	12 mo	12 mo	24 mo
New Parts Labeling	PN	PN	PN / SN barcoded

<b>Shipping &amp; Transportation &amp; Receiving</b> (Ref Section 4.6)	<b>APC 0/1</b>	<b>APC 2/3</b>	<b>APC 4</b>
Tamper evident packaging required Fundamental - sealed boxes / strapped pallets Improved - tamper evident seals upon shipment.	Fund.	Improved	Improved
Package tampering identified to be reported to IBM.	Y 24 hours	Y 24 hours	Y 24 hours
Parts sent to IBM require a detailed packing list to include PN/QTY, ship-to-address detail, carrier name, bill of lading / airbill, etc. numbers	Y	Y	N
Parts sent to IBM require a detailed packing list to include PN/SN detail, case no., date of shipment, ship-to-address detail, carrier name, bill of lading / airbill, etc. numbers	N	N	Y
Packing list to be received by IBM prior to arrival and no more than 48 hours after shipment	N	Y	Y
Receipt acknowledgment at supplier	PN Qty 24 hours	PN Qty 24 hours	PN/SN 8 hours
Overdue shipments reported	Y	Y	Y
Parts are not to be left unattended at supplier dock areas	-	-	Y

<b>Inventory Controls</b> (Ref Section 4.2)	<b>APC 0/1</b>	<b>APC 2/3</b>	<b>APC 4</b>
Root Cause Analysis on all variances	Financially determined	Financially determined	Y
Supplier conducts physical inventory and reports results to IBM	Annual	Annual	Qtrly
Variance reported to IBM	w/in 15 days	w/in 5 days	w/in 2 days
Shipping / Receiving / Counts / Audits / Variance records maintained on file by supplier	12 months	12 months	24 months by s/n
Logistic records reconciliation required to detect discrepancies	Annual	90 days	30 days
Supplier maintains proper separation of duties in inventory control process	Y	Y	Y
No sale of parts by the supplier to anyone other than IBM or its subsidiaries.	Y	Y	Y
Secondary Consignment of parts	IBM approval	IBM approval	IBM approval
Consumption Records based on order driving the consumption	N	N	Y

<b>Physical Security</b> (Ref Section 4.1)	<b>APC 0/1</b>	<b>APC 2/3</b>	<b>APC 4</b>
Supplier secures parts consistent with IBM Corporate Security's.	Y	Y	Y
IBM will conduct physical security audits at the supplier location.	Optional	Optional	Y
All must have a controlled reclamation and/or scrap process.	Y	Y	Authorized by IBM
All parts returned to IBM must have legible TIN's and/or part numbers, serial numbers.	PN/QTY	2:PN/QTY 3:PN&SN	PN & SN