BY ORDER OF THE COMMANDER
RAMSTEIN AIR BASE (USAFE)

RAMSTEIN AIR BASE INSTRUCTION
17-1203

16 JUNE 2025

Communications and Information

INFORMATION TECHNOLOGY ASSET MANAGEMENT (ITAM) AND ACCOUNTABILITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 86 CS/SCOSA

Certified by: 86 CS/CC
(Lt Col David L. Janowiak)

Pages: 24

This publication implements DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability*, DODI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*. It expands upon previously established guidance to further define actions, responsibilities, and expectations of Ramstein Air Force Base (RAB) Information Technology Asset Managers (ITAM), Base Software License Managers (BLSM), Unit Software License Managers (USLM), Unit Equipment Managers, and Ramstein network users. It applies to all military, civilian, and contract personnel operating, managing, maintaining, or controlling any Defense Property Accountability System (DPAS)-tracked information technology (IT) asset supported by AFNET and/or RAB. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command.

This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing, unit, delta or garrison level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternatively, to the

publication OPR for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Department of the Air Force. This publication requires the collection and/or maintenance of information protected by the Privacy Act of 1974 authorized by Title 10 U.S.C., Sec 9013, Secretary of the Air Force. Compliance with chapters **2**, **3**, and attachments **2**, **5**, and **6** is mandatory.

Chapter 1

PROGRAM OVERVIEW

1.1. Introduction.

1.1.1. This instruction implements processes necessary to perform Information Technology Asset Management (ITAM) for all Information Technology (IT) hardware operating on Ramstein Air Base's Air Force Information Networks (AFIN), including the Kaiserslautern Military Community (KMC) and associated Geographically Separated Units (GSUs).

1.2. Purpose.

1.2.1. The purpose of this instruction is to standardize procedures and establish best practices as it applies to conducting ITAM and Property Custodian (PC) interactions.

1.3. Scope.

1.3.1. The scope of ITAM encompasses business processes related to the asset management lifecycle including acquisition, receipt, acceptance, physical or automated inventory, transfer, management, disposal, and financial reporting.

1.3.2. This instruction applies to all Ramstein Air Base (RAB) users and supported GSU users.

1.3.3. All processes defined within this instruction apply to all IT hardware operating on both NIPRNet and SIPRNet, unless otherwise explicitly stated.

1.4. ITAM Terms and Definitions.

1.4.1. IT hardware refers to devices such as computing systems and/or network systems that process, store, and distribute data. This includes but is not limited to client computing systems, mice, keyboards, monitors, Keyboard Video Mouse (KVM) switches, Voice over Internet Protocol (VoIP) telephones, Video Teleconferencing (VTC) devices, mobile hotspots, networking equipment, printers, scanners, and fax machines.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. 86 CS ITAM Office will:

2.1.1. Be appointed by the host/tenant Accountable Property Officer (APO) to serve as an Equipment Control Officer (ECO) and Base Software License Manager (BSLM).

2.1.2. Be accountable for all accountable IT assets on RAB and supported GSUs, unless otherwise delegated.

2.1.3. Ensure the Defense Property Accountability System (DPAS) inventory provides management for all accountable IT hardware assets in accordance with this instruction.

2.1.4. Track appointment of Property Custodians (PC).

2.1.5. Track appointment of Unit Software License Managers (USLM).

2.1.6. Process the receipt, transfer and disposal of all accountable IT assets and complete necessary documentation to establish or relinquish custodial responsibility.

2.1.7. Assist PCs in determining the ownership, reassignment, or disposition of all found-on-base accountable IT assets.

2.1.8. Direct PCs to conduct annual inventories in accordance with DAFMAN 17-1203, para 2.3.7.3 and this instruction.

2.1.9. Provide PCs with labels for assets in accordance with DAFMAN 17-1203, para 2.6.1.4.

2.1.10. Provide inventory assistance in accordance with DAFMAN 17-1203, Attachment 4.

2.1.10.1. Conduct a network scan of all devices connected to the network, once per month.

2.1.10.2. Upload network scan results to the ITAM SharePoint page to assist PCs, IAW DAFMAN 17-1203 A4.3.2, in accomplishing inventories.

2.1.11. Implement and utilize a uniform device naming convention to aid in easily correlating network assets to the owning unit when performing network scans or any required quarantine actions.

2.1.12. Provide software license training for USLMs for managing licenses.

2.1.13. Direct USLMs annually, to initiate, collect, and provide to the 86 CS ITAM Office, unit baseline inventories for:

2.1.13.1. All non-enterprise software for all assets under their purview.

2.1.13.2. All enterprise software for all stand-alone assets under their purview.

2.1.14. Develop an annual spend plan to project for a 25% life cycle management of all NIPR and SIPR devices to meet the 4-year workstation life cycle management objective defined in DAFMAN 17-1203.

2.1.15. Work in tandem with 86 CS/SCXR and U-A A6/CR to properly project any unfunded requests required according to the spend plans created.

2.1.16. Host a quarterly PC working group to drive base-wide initiatives and strategic messaging for all supported units. Each working group shall have a virtual option for GSUs. If necessary, the quarterly PC working group may be held jointly with the quarterly UCR working group hosted by the 86 CS Wing Cybersecurity Office to streamline communication efforts.

2.2. Unit Accountable Property Officer (UAPO).

2.2.1. Organization commanders, or equivalent, shall serve as UAPO and are responsible for providing guidance and procedures to ensure adequate protection and oversight is afforded to safeguard IT assets under their control.

2.2.2. Will appoint at least one primary and one alternate PC per account in accordance with DODI 5000.64. The UAPO will ensure appointed PCs acknowledge their duties with handwritten or digital signatures, and the UAPO will ensure a copy of the documentation is provided to the 86 CS ITAM Office.

2.2.3. Will appoint at least one primary and one alternate USLM. The appointed USLMs may be the same members appointed as PCs.

2.3. Unit Property Custodians (PC).

2.3.1. At least one primary and one alternate PC per account will be appointed by the UAPO. There is no minimum rank requirement for PCs.

2.3.2. PCs shall be accountable for all assigned accountable IT hardware assets within their respective custodian accounts.

2.3.3. PCs will ensure individuals receiving accountable assets validate acceptance with signed documentation i.e., AF Form 1297 or locally developed receipt. PC will retain a copy of the signed document in their account folder on the 86 CS ITAM Office SharePoint site.

2.3.4. Will perform, at a minimum, an annual inventory of all accountable IT hardware assets within their respective custodian accounts in accordance with DAFMAN 17-1203, Attachment 4.

2.3.5. Will ensure all accountable assets have labels containing serial number, part number, manufacturer CAGE code, and PC account number affixed prior to being placed in service and verified during annual inventories.

2.3.6. Will ensure all accountable IT equipment shipments are sent to the 86 CS ITAM Office and will send notification via email to **86CS.SCOSA.ITAM@us.af.mil** of all incoming and outgoing shipments, transfers, donations, or turn-ins of assets.

2.3.7. Will provide appropriate documentation to the 86 CS ITAM Office to clear the account of equipment that was shipped to another base/location, transferred to another account, or turned into Defense Logistics Agency Disposition Services (DLADS).

2.3.8. Must be approved to out-process by their organization’s commander or equivalent and the 86 CS ITAM office.

2.3.9. Upon discovery of lost, stolen, damaged, or destroyed assets, PCs will perform actions outlined in **section 3.1.2.3**.

2.3.10. Must ensure hard drives are removed from assets prior to turn-in to DLADS.

2.3.11. Must ensure removed hard drives are sanitized IAW 86 CS ITAM Office procedures.

2.3.12. PCs will ensure their unit adheres to all 86 CS network vulnerability management guidance and policies.

2.3.12.1. Ensure each of their systems are online and configured to be successfully scanned with the vulnerability assessment tool (i.e. ACAS).

2.3.12.2. Ensure vulnerabilities identified are patched as requested by the 86 CS.

2.3.12.3. Ensure compliance with an endpoint security system (i.e. Trellix, Microsoft Defender for Endpoint, etc.).

2.3.12.4. Utilize the 86 CS Windows Deployment Services (WDS) server for all systems connected to any 86 CS owned network via a Remedy or ServiceNow IT trouble ticket submitted to the 86 CS imaging lab.

2.3.12.5. If declining to use the 86 CS WDS server, unit agrees to use the monthly updated image supplied by the 86 CS.

2.3.12.6. Provide written documentation outlining justification for any system requested to deviate from the outlined vulnerability management policies.

2.3.12.7. Ensure all NIPRNet and SIPRNet devices added to the 86 CS network adhere to the 86 CS System Naming Nomenclature.

2.4. Unit Software License Managers (USLM).

2.4.1. Serves as the unit level focal point for managing the coordination for installation and removal of software on IT assets under their purview. Generates requests or provides for validation of software to be installed or removed from unit systems.

2.4.2. Manages all software licenses owned by the organization.

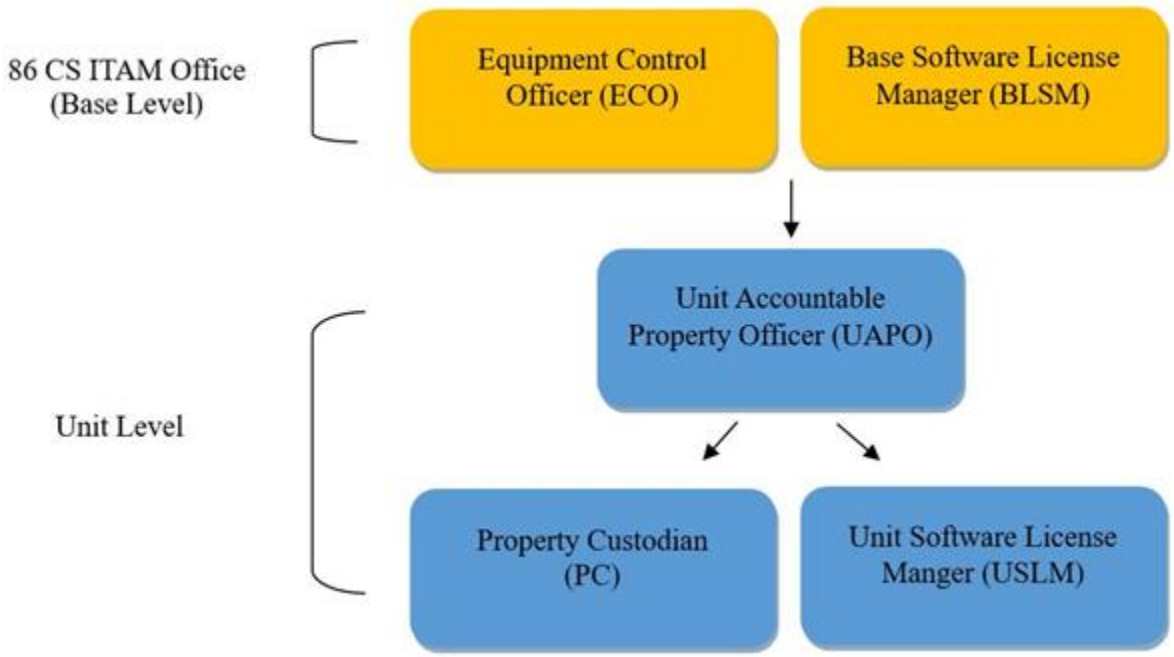
2.4.3. Submits a Cyberspace Infrastructure Planning System (CIPS) ticket for approval of all enterprise and non-enterprise software acquisitions through the 86 CS ITAM Office prior to purchasing software.

2.4.4. Establishes accountability of software licenses upon receipt of the invoice, maintains accountable records for the life of the asset, and retains records within their applicable USLM folder on the 86 CS ITAM SharePoint.

2.4.5. Conducts annual audits of all IT hardware under their purview to ensure no illegal/unauthorized software is installed.

2.4.6. Conducts annual and out-of-cycle inventories, if requested, of all software under their purview and retains inventory documentation within their applicable USLM folder on the 86 CS ITAM SharePoint.

Figure 2.1. Property (Physical) Accountability Roles Overview.



2.5. Accountability of IT Hardware.

2.5.1. Accountability of IT hardware resides with the organization's commander or equivalent and the appointed PCs. Physical and financial accountability takes place throughout the lifecycle of the asset and through disposal.

2.5.2. All IT hardware, both on and off the network, must be accounted for in DPAS.

2.5.3. Any asset recorded, tracked, and managed in DPAS must be inventoried at least annually.

2.5.4. PCs may utilize network scans to conduct their annual inventory. Monthly network scans are made available on the 86 CS ITAM SharePoint page.

2.5.5. Organizations with Special Access Program (SAP) assets must provide a digitally signed email from the organization's Information Systems Security Officer (ISSO) or Information Systems Security Manager (ISSM) stating the assets are accountable under the SAP inventory along with the asset's AF Identification (AFID) numbers. SAF/CNZC is responsible for issuing AF Identification (AFID) numbers for SAP IT systems in accordance with DAFMAN 17-1203, para 1.2.2.

2.5.5.1. SAP items will not be tracked in DPAS but will be labeled with the assigned AF Identification (AFID) number and a notice stating, "This item is not tracked in DPAS".

2.6. Staff Assistance Visits (SAV).

2.6.1. The 86 CS ITAM Office will conduct random inspections to ensure PC accounts are within compliance.

2.6.2. 86 CS ITAM inspectors will:

2.6.2.1. Utilize questions derived from DAFMAN 17-1203 to assess account compliance and PC competence.

2.6.2.2. Select five (5) IT hardware assets, on site, at random and verify that they are on the applicable organization's PC account.

2.6.2.3. Select five (5) serial numbers on the applicable organization's DPAS inventory list and attempt to physically locate account for the assets.

2.6.2.4. Assign an overall SAV characterization of "Satisfactory" or "Unsatisfactory".

2.6.3. "Satisfactory" SAV characterization. If no significant issues are identified during the SAV, the 86 CS ITAM inspector will draft the report, sign, and route to the PC for their signature. PC will sign the report and promptly return it to the ITAM Office to be filed in PC's account folder.

2.6.4. "Unsatisfactory" SAV characterization. If any of the inspected areas are found to be unsatisfactory, i.e. assets are unable to be located or assets are found on site that are not on the proper PC account, the SAV will be deemed "Unsatisfactory". The inspector will draft the report, sign, and route to the PC for their signature. PC will sign the report and promptly return to the ITAM office within 5 duty days. The report will then be held by the ITAM Office for 15 calendar days to allow the PC to rectify the identified issues.

2.6.4.1. If the PC rectifies the issues within 15 calendar days, the SAV report will be updated to indicate items corrected and finalized assessment characterization (Note: initial "Unsatisfactory" characterization will remain on page 1 of the report and a finalized "Satisfactory" characterization will be placed after the 2nd indorsement on the signature page). Report will then be signed by 86 CS ITAM inspector and forwarded to the 86 CS/CC (or designated official) for acknowledgment and signature. Once signed, the report will be returned to the ITAM office; a copy of the report will be routed to the PC and stored in the PC's account folder.

2.6.4.2. If the PC does NOT rectify the issues within 15 calendar days, the SAV report will be finalized as an "Unsatisfactory" assessment and the PC account will be locked.

2.6.4.2.1. The report will be signed by 86 CS ITAM inspector and routed to the PC's organization commander (or equivalent) for situational awareness and to the 86 CS/CC (or designated official) for acknowledgment and signature. Once signed, the report will be returned to the ITAM office; a copy of the report will be routed to the PC and stored in the PC's account folder.

2.6.4.2.2. The PC will be required to provide the status of the corrective actions under way and include the estimated completion date(s) in the form of a Plan of Action and Milestones (POA&M), to the ITAM Office every 30 days until the item(s) is closed. The POA&M must address all deficiencies identified in the SAV and be endorsed by the PC's organization commander (or equivalent).

2.6.4.2.3. The PC will then be required to accomplish the account's full inventory and/or applicable documentation to account for the asset loss, gain, or program discrepancy before the ITAM Office will unlock the PC's account.

2.7. Procurement of IT Hardware.

2.7.1. Before purchasing any IT hardware defined in **paragraph 1.4.1**, the following must be met:

2.7.1.1. A CIPS ticket must be submitted and approved through the Ramstein Air Base CIPS SharePoint.

2.7.1.2. All purchases of client computing systems and monitors must utilize the Client Computing Solutions III (CCS-3) program. The CCS-3 releases a Quantum Enterprise Buy (QEB) catalog bi-annually with approved assets.

2.7.1.2.1. If unable to utilize the CCS-3 program, requesting organization must receive a signed waiver from the USAFE-AFAFRICA A6 Designated Waiver Authority, see **Attachment 2**.

2.7.1.3. All other purchases of IT hardware to include those waived by the USAFE-AFAFRICA A6 Designated Waiver Authority must be made via the Second-Generation IT (2GIT) buying program using the General Services Administration (GSA) AF Advantage Portal.

2.7.1.4. The purchasing organization's PC account must be compliant and in good standing. All PC accounts that are non-compliant will be locked and will not be approved to purchase new IT hardware until the account is brought into compliance.

2.7.1.5. All purchases must include specific "Ship To" and "Mark For" information. This will alleviate problems with the receipt and acceptance processing of new IT hardware.

2.7.1.5.1. "Mark For" information will contain the purchasing PCs name, unit, and PC account number, and may contain Contract Number Purchase Order Number Address, Phone Number, E-mail Address, Resource Advisor Name, and organization's commander or equivalent.

2.7.1.5.2. "Ship To" information will contain the complete 86 CS ITAM Office delivery address: 86 CS/SCOSA (Attn: *PC ACCOUNT NUMBER/PC NAME*) BUILDING (GEBAUDE) 2126, DOOR 4 RAMSTEIN AB (FLUGPLATZ), GERMANY, 66877.

2.7.2. PCs must inform the 86 CS ITAM Office via email at **86CS.SCOSA.ITAM@us.af.mil** of any large shipments so pre-arrangements can be made to ensure temporary storage space is available.

2.8. Receipt of IT Hardware.

2.8.1. When IT hardware shipments have been received to the ITAM warehouse, ITAM will notify the applicable PCs within 5 business days of delivery.

2.8.1.1. PCs with compliant accounts will be authorized to pick up their IT hardware and are expected to do so within 10 business days of initial notification of the shipment arrival.

2.8.1.2. PCs with non-compliant or "locked" accounts, not in good standing, will not be authorized to pick up their accountable IT hardware. PCs and their commander (or equivalent) will be notified of the delivery and actions required to get their account into

good standing. If the required actions are not taken within 45 days, PCs risk forfeiting ownership of the new equipment.

2.8.2. Due to limited warehouse space, 86 CS ITAM Office cannot store PC-allocated equipment for extended periods of time. PCs who fail to pick up their IT hardware, both newly delivered assets and assets under maintenance, in a timely manner, risk forfeiting ownership of the equipment.

2.8.2.1. **10 Days After Initial Pickup Notification:** If items have not yet been picked up by the purchasing PC, the ITAM office will notify the PC's organization commander, or equivalent, and 86 CS leadership of the organization's failure to pick up the equipment.

2.8.2.2. **30 Days After Initial Pickup Notification:** If items have not yet been picked up by the purchasing PC, the ITAM office will again, notify the PC's organization commander, or equivalent, and 86 CS leadership of the organization's failure to pick up the equipment. Organizations will also be notified of their pending forfeiture of ownership of the equipment.

2.8.2.3. **45 Days After Initial Pickup Notification:** If items have not yet been picked up and no prior arrangements or agreements have been made with the ITAM office, all equipment will be considered "abandoned" and will become property of 86 CS ITAM office. ITAM will reallocate assets as needed.

2.8.3. Prior to releasing IT hardware to the applicable PC, accountability will be established by formal receipt and/or acceptance in DPAS.

Chapter 3

PC ACCOUNT COMPLIANCE AND NON-COMPLIANCE

3.1. PC Account Compliance Requirements.

3.1.1. The ITAM office uses a last-day-of-the-month policy for annual due dates pertaining to PC account compliance requirements. This means, annual requirements will be due 1 year from the month they were previously signed. For example, if an annual inventory was signed on 12 July 2024, the inventory will remain in compliance until 31 July 2025.

3.1.2. PCs must conduct a physical inventory of all IT Hardware on their account(s) at least once annually. Upon completion, the DPAS inventory list must be signed by the PC(s) conducting the inventory, the organization's commander (or equivalent), and sent to the 86 CS ITAM Office by the last day of the month that it is due.

3.1.2.1. PCs must ensure gains or losses against the inventory list are documented and reconciled.

3.1.2.2. If IT hardware is found that is not on the inventory list, the PC must accomplish Found on Base (FOB) documentation for the asset(s). The FOB Form, as seen in **Attachment 6**, can be found on the ITAM SharePoint page.

3.1.2.3. If IT hardware is lost, stolen, damaged, or destroyed, the PC must:

3.1.2.3.1. Notify their organization's commander, or equivalent, and the 86 CS ITAM Office within 5 business days.

3.1.2.3.2. Report the loss of any IT hardware asset with persistent storage to the 86 AW Wing Cybersecurity Office (WCO).

3.1.2.3.3. Utilize the 86 Comptroller Squadron (CPTS) Report of Survey (ROS) SharePoint page at **https://usaf.dps.mil/sites/86WSA/CPTS/SitePages/ROS.aspx** or contact the 86 CPTS Financial Liability Investigation (FLI) office at **kmc.rosmanager@us.af.mil** within 5 business days to determine if an FLI, also known as an ROS, is required. It is important to note that the terms, "ROS" and "FLI", are used interchangeably depending on which resource you are referencing.

3.1.2.3.3.1. If an FLI is initiated and the PC account inventory is coming due, annotate the items included in the FLI next to the items on the account inventory list, sign the inventory, and send it to the 86 CS ITAM Office. This action will allow the PC account to remain "compliant" while the FLI, an often-lengthy process, is being conducted.

3.1.3. When appointed, PCs must complete Initial PC Training found on the ITAM SharePoint page. Once complete, PCs must digitally sign the training certificate and upload it to their applicable folder on the ITAM SharePoint page.

3.1.3.1. PC Training is only required once, upon initial appointment. However, since new direction, processes or requirements could be released at any given time, PCs must regularly check the announcements section of the ITAM SharePoint page and/or familiarize themselves with the most current version of the PC Training slides if a year or more has passed since their initial training.

3.1.4. PC accounts must have a current appointment letter on file with the 86 CS ITAM Office. Appointment letters are deemed "current" if the PCs listed are still accurate and are continuing to carry out their appointed duties regardless of appointment letter date or signature authority. 86 CS reserves the right to request updated appointment letters as needed.

3.1.5. A compliant PC account is defined as an account that has a current, signed inventory list dated within the past 12 months, a current appointment letter, and training certificates for both PCs on file with the 86 CS ITAM Office.

3.1.6. A non-compliant PC account is defined as an account that does not have 1 or more of the documents, as defined in **paragraph 3.1.5**, on file with the 86 CS ITAM Office.

3.2. Non-Compliant Accounts.

3.2.1. If a PC account fails to meet the criteria defined in **paragraph 3.1.5** to maintain account compliance, the following actions will take place:

3.2.1.1. **1 Day Past Due:** Applicable PCs will be notified that their account is now non-complaint and locked by the 86 CS ITAM Office. Accounts that have been locked are prohibited from:

3.2.1.1.1. Receiving assets or transferring assets to other accounts.

3.2.1.1.2. Receiving any IT technology refresh equipment.

3.2.1.1.3. Ordering new accountable IT assets through CCS-3 or GSA Advantage.

3.2.1.1.4. Receiving purchase authorizations routed through the 86 CS CIPS SharePoint.

3.2.1.1.5. Receiving prior-ordered IT assets delivered to the 86 CS ITAM warehouse.

3.2.1.1.6. Conducting asset turn-ins to Defense Logistics Agency (DLA).

3.2.1.1.7. Out-Processing PCs via Virtual MPF.

3.2.1.2. **30 Days Past Due:** Organization's commander or equivalent, of applicable PC accounts will be notified of non-compliance. A Plan of Action and Milestones (POA&M) will be required from the PCs detailing:

3.2.1.2.1. Reason for non-compliance.

3.2.1.2.2. Steps being taken to achieve account compliance.

3.2.1.2.3. Projected get-well date.

3.2.1.3. **60 Days Past Due:** 86 CS will suspend all PC accounts owned by the offending organization, if applicable. Additionally, 86 CS will suspend support for all CIPS work orders, to include new and existing communications upgrades or installations, for the offending organization. The CIPS work orders will be placed in Pending Customer Action (PCA) status. The offending organization's commander or equivalent will be notified of the continued non-compliance and 86 CS's pause on IT support.

3.2.1.3.1. If CIPS support is deemed mission critical by the offending unit, an Exception to Policy (ETP) MFR will be required. **See Attachment 3**.

3.2.1.3.1.1. The MFR must list the specific work order number(s), a mission

impact justification, and must be signed by the offending organization's commander or equivalent.

3.2.1.3.1.2. The signed MFR will be routed through the ITAM Office to the 86 CS/CC (or designated official) for approval.

3.2.1.4. **90 Days Past Due:** 86 CS will continue to suspend support for all CIPS work orders unless there is a prior approved ETP for the offending organization. The offending organization's commander and group commander or equivalents will be notified of the continued non-compliance and 86 CS's pause on IT support.

3.2.1.5. **120 Days Past Due:** 86 CS will suspend support for all open and incoming virtual Enterprise Service Desk (vESD), Remedy, ServiceNow trouble tickets, incidents, and requests, collectively referred to as IT trouble tickets from this point forward. Tickets will be placed in PCA or equivalent status. All CIPS work orders without a prior approved ETP will be closed out. The offending organization will be allowed to resubmit requests after ITAM account(s) have been brought back into compliance. The offending organization's commander and group commander or equivalents will be notified of the continued non-compliance.

3.2.1.5.1. If IT trouble ticket support is deemed mission critical by the offending unit, an ETP MFR will be required. **See Attachment 4**.

3.2.1.5.1.1. Not Utilized

3.2.1.5.1.2. The MFR must list the specific ticket number(s), a mission impact justification, and must be signed by the offending organization's commander or equivalent.

3.2.1.5.1.3. The signed MFR will be routed through the ITAM Office to the 86 CS/CC (or designated official) for approval.

3.2.1.6. **180 Days Past Due:** All open IT trouble tickets that do not have a prior approved ETP will be closed out. The offending organization may resubmit requests after ITAM account(s) have been brought back into compliance. The offending organization's commander, group commander, and wing commander or equivalents will be notified of the continued non-compliance and 86 CS's pause on IT support.

3.2.1.6.1. Only high priority IT trouble tickets with approved ETP MFRs will be fielded and worked. See **paragraph 3.2.1.5.1**.

3.3. Right to Refuse Communications Support for End-of-Life (EoL) IT Equipment.

3.3.1. To preserve the reliability and security of the network, the 86 CS reserves the right to refuse communications support for out-of-warranty or EoL IT equipment. This parameter is aimed at eliminating potential network vulnerabilities that may arise from the continued use of such equipment which could compromise the overall security and functionality of the network.

3.3.2. If replacement of equipment is deemed necessary, users will coordinate with their respective PCs to facilitate the issuance of new systems that meet the necessary standards for network support and security.

Chapter 4

CORRESPONDANCE WITH THE ITAM OFFICE

4.1. SharePoint.

4.1.1. The 86 CS SCOS ITAM Office has established a customer-friendly SharePoint page to provide PCs with training, common documents, procedures, answers to frequently asked questions, and more. The ITAM SharePoint page also houses all PC account(s) folders, as tracked by the ITAM office. PCs are expected to utilize the ITAM SharePoint page to answer common questions, find common documents, review PC training and/or determine requirements before attempting to contact the ITAM office via email or phone.

4.2. Email Correspondence.

4.2.1. Requests and inquiries not addressed on the ITAM SharePoint page, or document submissions should be sent to the ITAM organizational email box, **86CS.SCOSA.ITAM@us.af.mil**. All correspondence to this address will be responded to within 3 business days.

4.2.2. To help further expedite email responses, all emails sent to the organizational email box should utilize standardized subject lines beginning with the account number, followed by the action being requested or overall topic of the message. Some examples can be seen below:

4.2.2.1. **Email Subject: "Account ####//Transfer Request"**

4.2.2.1.1. Used when requesting an asset transfer between PC accounts. Account number initiating the transfer will be used in the subject line.

4.2.2.1.2. PCs must first ensure that both the losing and gaining accounts are in compliance, as defined in **paragraph 3.1.5**, before initiating this request.

4.2.2.1.3. PCs must utilize the "Ramstein IT Equipment Transfer Form". **See Attachment 5**.

4.2.2.2. **Email Subject: "Account ####//Inventory Request"**

4.2.2.2.1. Used when requesting a new account inventory for PC transfers or other account validation reasons.

4.2.2.2.2. PCs must specify whether they are requesting a loss-gain inventory (for account turnover to new PC), an annual inventory, or an unofficial inventory.

4.2.2.3. **Email Subject: "Account ####//Update Account"**

4.2.2.3.1. Used when providing new appointment letters, inventories, training certificates, etc. to the ITAM office.

4.2.2.4. **Email Subject: "Account ####/FOB"**

4.2.2.4.1. Found on Base (FOB) forms must have the applicable serial numbers, makes, and models listed and be digitally signed by the PC.

4.2.2.4.2. PCs must utilize the "Ramstein IT Found on Base Form". **See Attachment 6**.

4.2.2.4.3. After FOB assets are added to the PC's account, the 86 CS ITAM office will sign and send a digital copy to the PCs and place a copy in the applicable account folder on SharePoint.

ADRIENNE L. WILLIAMS, Brig Gen, USAF
Commander, 86th Airlift Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability,* 13 September 2022

DODI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, 10 June 2019

Ramstein Air Base Cyberspace Infrastructure Planning System (CIPS) SharePoint, **https://usaf.dps.mil/sites/86CS/SCO/SCOC/CIPS/SitePages/Home.aspx**

86th Communications Squadron Asset Management Portal, **https://usaf.dps.mil/sites/86CS/SCO/SCOS/SitePages/86TH-COMMUNICATION-SQUADRON-ASSET-MANAGEMENT-PORTAL.aspx**

86th Comptroller Squadron (CPTS) Report of Survey (ROS), **https://usaf.dps.mil/sites/86WSA/CPTS/SitePages/ROS.aspx**

Prescribed Forms

AF Form 1297, *Temporary Issue Receipt*

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

2GIT—Second-Generation Information Technology

ACAS—Assured Compliance Assessment Solution

AFI—Air Force Instruction

AFID—Air Force Identification

AFIN—Air Force Information Network

AFRIMS—Air Force Records Information Management System

APO—Accountable Property Officer

BSLM—Base Software License Manager

CCS-3—Client Computing Solutions III

CIPS—Cyberspace Infrastructure Planning System

CPTS—Comptroller Squadron

CS—Communications Squadron

DLADS—Defense Logistics Agency Disposition Services

DPAS—Defense Property Accountability System

ECO—Equipment Control Officer

ETP—Exception to Policy

FLI—Financial Liability Investigation

FOB—Found on Base

GSA—General Services Administration

GSU—Geographically Separated Unit

ISSM—Information Systems Security Manager

ISSO—Information Systems Security Officer

IT—Information Technology

ITAM—Information Technology Asset Management

KVM—Keyboard Video Mouse

PC—Property Custodian

POA&M—Plan of Action and Milestones

QEB—Quantum Enterprise Buy

RAB—Ramstein Air Base

RDS—Records Disposition Schedule

ROS—Report of Survey

SAP—Special Access Program

SAV—Staff Assistance Visit

U-A—United States Air Forces in Europe-Air Forces Africa

UAPO—Unit Accountable Property Officer

UCR—Unit Cybersecurity Representative

USLM—Unit Software License Manager

vESD—virtual Enterprise Service Desk

VoIP—Voice over Internet Protocol

VTC—Video Teleconferencing

WCO—Wing Cybersecurity Office

WDS—Windows Deployment Server

Office Symbols

86 CS/SCOSA—86 Communications Squadron/Information Technology Asset Management Office

86 CS/SCXR—86 Communications Squadron/Resource Advisor Office

AF/RE—Air Force Reserve

SAF/AA—The Administrative Assistant to the Secretary of the Air Force

SAF/CNZC—Office of the Chief Information Security Officer

U-A A6/CR—United States Air Forces in Europe-Air Forces Africa Communications Directorate/Contracts & Resources

Terms

Accountable Forms—Forms that the Department of the Air Force stringently controls and which cannot be released to unauthorized personnel since the misuse of accountable forms could jeopardize DoD security or could result in fraudulent financial gain or claims against the government. The unit receiving a request for accountable forms will inform the requester of this guidance.

Administrative Change—Change that does not affect the subject matter, content, authority, purpose, application, and/or implementation of the publication (e.g., changing the AO name, office symbol(s), fixing misspellings, etc.).

Approval Authority—Senior leader responsible for contributing to and implementing policies and guidance/procedures pertaining to his/her functional area(s) (e.g., heads of functional two-letter offices).

Authentication—Required element to verify approval of the publication; the approval official applies his/her signature block to authenticate the publication. The signature block includes the official’s name, rank, and title (not signature).

Attachment 2

MFR: WAIVER REQUEST FROM USING CLIENT COMPUTING SOLUTIONS III (CCS-3)

Figure A2.1. MFR: WAIVER REQUEST FROM USING CLIENT COMPUTING SOLUTIONS III (CCS-3).

DD Mmmm YYYY

MEMORANDUM FOR MAJCOM/A6/Field Command Representative
ATTENTION: *Designated Waiver Authority*

FROM: *Requesting Unit*/CC

SUBJECT: Waiver Request from using Client Computing Solutions III (CCS-3)

1. Per AFMAN 17-1203, we request a waiver for the purchase of:

   a. Item:

   b. Item Description:

   c. Estimated Price (each and total):

2. Waiver Reason/Rationale:

3. Operational/Supply Chain Risks, Other Considerations:

4. Proposed Source:

5. If you have any questions or concerns, please contact first.last@us.af.mil or DSN: ###-####.

FIRST MI. LAST, Rank, USAF
Commander

1st Ind, MAJCOM/A6 or Field Command Representative

MEMORANDUM FOR *Requesting Unit*/CC

Request for waiver is approved/disapproved.

FIRST MI. LAST, Rank, USAF
Designated Waiver Authority

Attachment 3

MFR: EXCEPTION TO POLICY FOR CIPS SUPPORT

Figure A3.1. MFR: EXCEPTION TO POLICY FOR CIPS SUPPORT.

DD Mmmm YYYY

MEMORANDUM FOR 86 CS/CC

FROM: *Requesting Unit*/CC

SUBJECT: Exception to Policy for CIPS Support

1. This is to acknowledge that *ITEC ACCOUNT #* is locked and non-compliant. Due to the mission requirement, I am requesting 86 CS to provide support for *CIPS #(s).*

2. Mission Requirement:

3. Mission Justification:

4. If you have any questions or concerns, please contact first.last@us.af.mil or DSN: ###-####.

FIRST MI. LAST, Rank, USAF
Commander

Attachment 4

EXCEPTION TO POLICY FOR IT TICKET SUPPORT

Figure A4.1. MFR: EXCEPTION TO POLICY FOR IT TICKET SUPPORT.

DD Mmmm YYYY

MEMORANDUM FOR 86 CS/CC

FROM: *Requesting Unit*/CC

SUBJECT: Exception to Policy for IT Ticket Support

1. This is to acknowledge that *ITEC ACCOUNT #* is locked and non-compliant. Due to the mission requirement, I am requesting 86 CS to provide support for *Remedy/ServiceNow ticket #(s).*

2. Mission Requirement:

3. Mission Justification:

4. If you have any questions or concerns, please contact first.last@us.af.mil or DSN: ###-####.

FIRST MI. LAST, Rank, USAF
Commander

Attachment 5

RAMSTEIN IT EQUIPMENT TRANSFER FORM

Figure A5.1. RAMSTEIN IT EQUIPMENT TRANSFER FORM.

RAMSTEIN IT EQUIPMENT TRANSFER FORM

This form is used to transfer IT hardware between DPAS Accounts. Property Custodians (PC) must first ensure that both the losing and gaining accounts are in compliance (current inventory, appointment letter, and PC training) before submitting this transfer request to 86 CS ITAM Office. The information required on this form can be obtained from the DPAS inventory listing or the asset's barcode label. ALL FIELDS BELOW MUST BE FILLED IN!

ITEM	SERIAL NUMBER	MANUFACTURER	MODEL / DESCRIPTION	NEW LOCATION	
				Bldg	Rm #
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					

As the Unit Software License Manager (USLM), I have made all applicable updates to my software license inventory to account for any software licenses loaded to the above systems.

	LOSING PROPERTY CUSTODIAN	GAINING PROPERTY CUSTODIAN
ACCOUNT NUMBER:		
ORG/OFFICE SYMBOL:		
PC RANK / NAME:		
SIGNATURE:		
DATE:		

ITAM OFFICE USE ONLY

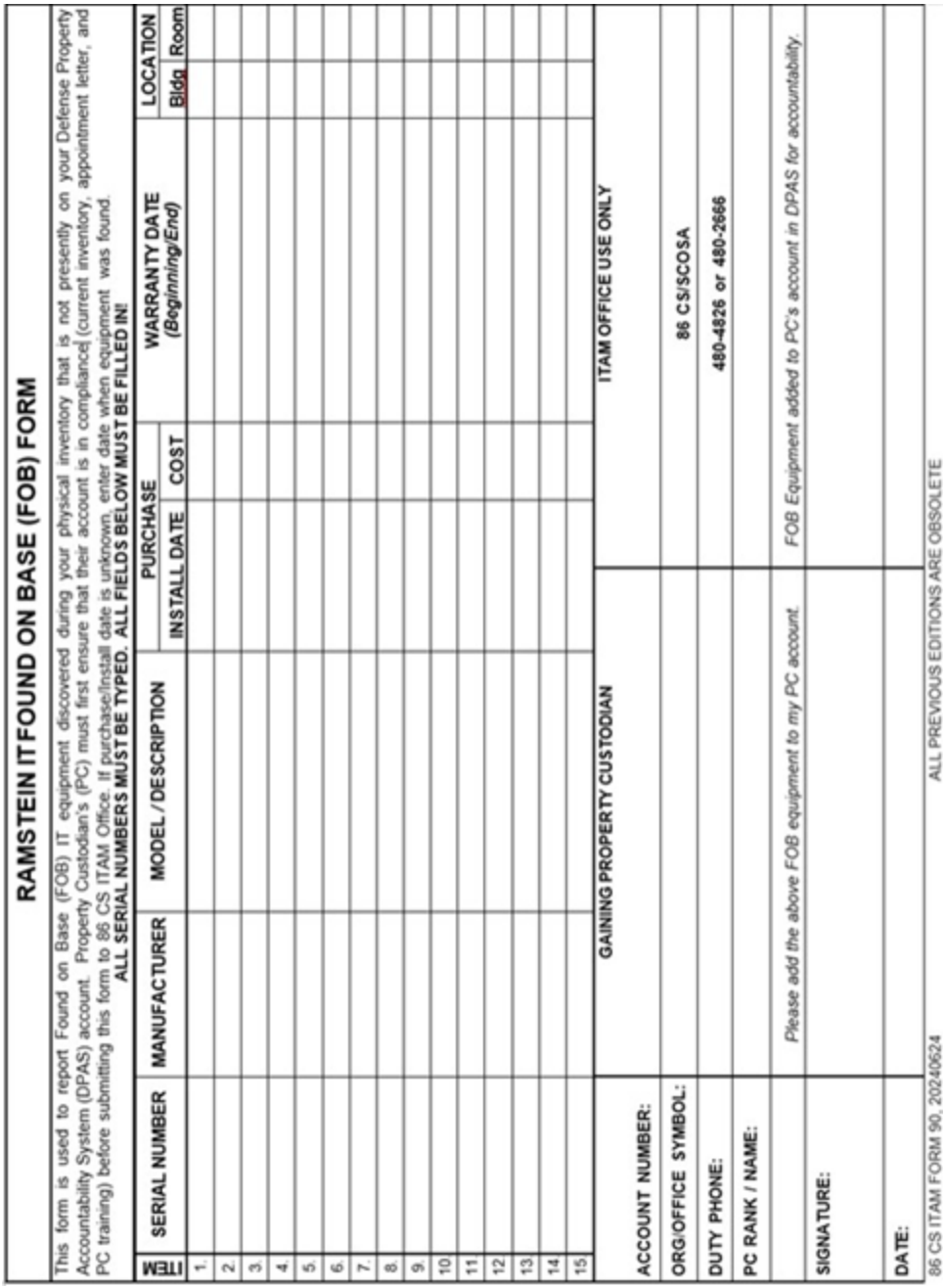
PROCESSED BY: DATE:

86 CS ITAM FORM 96, 20240624 PREVIOUS EDITIONS OBSOLETE

Attachment 6

RAMSTEIN IT FOUND ON BASE (FOB) FORM

Figure A6.1. Ramstein It Found on Base (FOB) Form.



RAMSTEIN IT FOUND ON BASE (FOB) FORM

This form is used to report Found on Base (FOB) IT equipment discovered during your physical inventory that is not presently on your Defense Property Accountability System (DPAS) account. Property Custodian's (PC) must first ensure that their account is in compliance (current inventory, appointment letter, and PC training) before submitting this form to 86 CS ITAM Office. If purchase/install date is unknown, enter date when equipment was found.
ALL SERIAL NUMBERS MUST BE TYPED. ALL FIELDS BELOW MUST BE FILLED IN!

ITEM #	SERIAL NUMBER	MANUFACTURER	MODEL / DESCRIPTION	PURCHASE		WARRANTY DATE *(Beginning/End)*	LOCATION	
				INSTALL DATE	COST		Bldg	Room
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10								
11								
12								
13								
14								
15								

GAINING PROPERTY CUSTODIAN	ITAM OFFICE USE ONLY
ACCOUNT NUMBER:	
ORG/OFFICE SYMBOL:	86 CS/SCOSA
DUTY PHONE:	480-4826 or 480-2666
PC RANK / NAME:	
Please add the above FOB equipment to my PC account	*FOB Equipment added to PC's account in DPAS for accountability*
SIGNATURE:	
DATE:	

86 CS ITAM FORM 90, 20240624 ALL PREVIOUS EDITIONS ARE OBSOLETE