EXTERNAL CONTRACTOR SUPPORT

Information Assurance Control Agreement

ENVIRONMENTAL RESOURCES PROGRAM INFORMATION MANAGEMENT SYSTEM

(ERPIMS) ERPTOOLS X

THIS PAGE INTENTIONALLY BLANK

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to satisfy the Information Assurance (IA) controls mandated by Department of Defense (DoD) Instruction (DoDI) 8500.2, Information Assurance and the Federal Information Security Management Act (FISMA). Responsibility for procedural and administrative security is shared between the service provider (AFCEE) and the supported entity contracting for the service (ERPIMS data) and must meet the DISA Best Security Practices**.** This IA Control Agreement is specifically written for a Mission Assurance Category Level III (MAC III) system that processes sensitive data as defined in DoDI 8500.2.

1.2 IA Control Compliance Procedures

It is the responsibility of the contractor to ensure that all IA controls listed in this document are identified as implemented or not implemented according to the guidance provided in this document.

1.3 Procedures for Non-Compliance

The contractor company will ensure 100% compliance with implementation of security actions of IA controls defined in this document. When IA control compliance falls below this threshold, associated ERPIMS user accounts will be deactivated. ERPIMS Program Management Office (PMO) will work with the customer to resolve problems and report progress to the contracting officer (CO).

2 Local ERPIMS/ERP Tools X Contractor Base Site and/or Laboratory

2.1 Description of Services Provided

The ERPTOOLS X program is client-based software residing at contactor sites (commercial), including laboratories.

The contractor company using the ERPTools X software is responsible for implementing the following IA controls**. For additional details regarding verification and guidance, please reference the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) validation procedures. DIACAP validation procedures are available upon request.**

Table 2.1.1: CODB-1 Data Backup Procedures

Number	Name	Subject Area	Impact Code
CODB-1	Data Backup Procedures	Continuity	Low
Implementation Guidance			
This guidance is written for system administrators with backup privileges: 1. Ensure that site(s) is/are designated for storage of backup/recovery media at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level. 2. Label backup media with the appropriate information, including system identifier, classification or sensitivity labeling, and a date/time stamp.			
Reference			
DoD Directive 3020.26, Defense Continuity Program, 08 September 2004			

Q&A
Q: My company does not currently back up our data and does not have available backup servers or systems. What can I do? A: Backing up data can be automated or manual. In addition, backing up data does not necessarily mean purchasing expensive equipment with large storage capabilities. Data can easily be backed up (saved) onto an External Hard drive via a USB connection. Folders created on the External Drive can be named with the "system identifier, classification level, and a date/time stamp. Please see the example below. Folder within External Drive: H:\myserver_fouo_14_mar_1300_backup

Table 2.1.2: ECAR-2 Audit Record Content – Sensitive Systems

Number	Name	Subject Area	Impact Code
ECAR-2	Audit Record Content – Sensitive Systems	Enclave Computing Environment	Medium
Implementation Guidance			
1. Enable system log monitoring (e.g., Microsoft Windows Event Logging).			
Reference			
Q&A			
Q: My company would like to enable system log monitoring on our ERPTools X systems. Is this an easy process? How can I accomplish this task and be compliant with ECAR-2? **A:** *ECAR-2 requires simple audit logs to be enabled. Here are some examples audit logs requiring enabling on your system. If the following are enabled, you are compliant.* • *User ID* • *Successful and unsuccessful attempts to access security files* • *Date and time of the event* • *Success or failure of event* • *Successful or unsuccessful logon attempts* • *Denial of Service due to excessive number of logon attempts* *Your system administrator can assist you with enabling auditing on your system.*			

Table 2.1.3: ECCR-1 Encryption for Confidentiality (Data at Rest)

Number	Name	Subject Area	Impact Code
ECCR-1	Encryption for Confidentiality (Data at Rest)	Enclave Computing Environment	Medium
Implementation Guidance			
1. Encrypt data at rest (e.g., encrypt hard drive). Note: AFCEE will implement encryption of data at rest within the ERPTools X application in the next scheduled release.			
Reference			
Q&A			

Q: My company has highly skilled and trained Information Assurance (IA) personnel on staff, but does not have the capability of "encryption for Confidentiality (data at rest)" on current systems. What can I do?

A: *ECCR-1 (Encryption of Confidentiality or data at rest) will be implemented in the next ERPTools X release.* ***Please disregard this control at this time.***

Table 2.1.4: ECLO-1 Logon

Number	Name	Subject Area	Impact Code
ECLO-1	Logon	Enclave Computing Environment	Medium

Implementation Guidance

1. Successive logon attempts on workstations/laptops are controlled using one or more of the following:
   - Access is denied after multiple unsuccessful logon attempts.
   - The number of access attempts in a given period is limited.
   - A time-delay control system is employed.

Reference

8500.02 Information Assurance Implementation, February 6, 2003, Page 96

Q&A

Q: My laptop containing the ERPTools X Application doesn't require a username to logon to the laptop. I asked my administrator to create a user account on the laptop and now I have to use a username and password to login after turning the laptop on. Did I meet the requirement?

A: *ECLO-1 (Logon Controls for SUB information systems) has two subcategories that must be met. You met the first requirement by requiring a username and password for access to the system, but still need to implement access to the system/laptop denied after 3invalid login attempts or a time-delay controls system enabled; meaning after 3 invalid login attempts, the system will not allow another login attempt for a set period of time (i.e. 30 minutes). Please see the example below.*

For Windows 7, please see the following instructions:

With administrative privileges, go to: Control Panel → Administrative Tools → Local Security Policy → Account Policy → Account Lockout Policy. The first two out of the three settings can be configured: 1) Account Lockout Duration i.e. 30 minutes, 2) Account Lockout threshold i.e. 3.

Table 2.1.5: ECML-1 Marking and Labeling

Number	Name	Subject Area	Impact Code
ECML-1	Marking and Labeling	Enclave Computing Environment	High

Implementation Guidance

2. Label backup media with the appropriate information, including system identifier, classification or sensitivity labeling, and a date/time stamp.
3. Label/mark data output with appropriate classification.

Reference

Note: Reports or Media containing Location Identification (LOCID), Location Proximity (LPRCODE), North Coordinate (NCOORD), East Coordinate (ECOORD) and Location Description (LOCDESC) should be marked as "FOR OFFICIAL USE ONLY".

Q&A

Q: Should all of my media, to include CD's, DVD's, hard drives, external drives, etc., containing ERPTools X

data/information be marked with the date and classification?

A: *Yes. Mark all media with the date and "UNCLASSIFED/FOUO". This can be as simple as a label or marker (Sharpie). Printed documents should have the "UNCLASSIFED/FOUO" classification on the top and bottom of the page.*

Table 2.1.6: ECNK-1 Encryption for Need-to-Know

Number	Name	Subject Area	Impact Code
ECNK-1	Encryption for Need-to-Know	Enclave Computing Environment	Medium
Implementation Guidance			
1. Encrypt data at rest. (e.g., encrypt hard drive) Note: AFCEE will implement encryption of data at rest within the ERPTools X application in the next scheduled release.			
Reference			
Q&A			
Q: My company has highly skilled and trained Information Assurance (IA) personnel on staff, but do not have the capability of "encryption for need to know" on current systems. What can I do? **A:** *ECNK (Encryption for need-to-know) will be implemented in the next ERPTools X release.* ***Please disregard this control at this time.***			

Table 2.1.7: ECRR-1 Audit Record Retention

Number	Name	Subject Area	Impact Code
ECRR-1	Audit Record Retention	Enclave Computing Environment	Medium
Implementation Guidance			
1. Activate audit logging for security-significant events. 2. Ensure settings allow logging for 1 year minimum retention. 3. Maintain backups in a secure environment.			
Reference			
8500.02 Information Assurance Implementation, February 6, 2003, Page 97			
Q&A			
Q: How do I enable logging for security significant events? **A:** ***For Windows 7, please see the following instructions:*** *With administrative privileges, go to: Control Panel → Right Click on Computer → Manage → Event Viewer → Windows Logs → Security → Right Click Properties → Choose Archive log when full do not overwrite events.* *Note: Event logs will be stored under C:/Windows/System32/Winevt/Logs*			

Table 2.1.8: ECTP-1 Audit Trail Protection

Number	Name	Subject Area	Impact Code
ECTP-1	Audit Trail Protection	Enclave Computing Environment	Medium
Implementation Guidance			
1. Contents of audit trails are protected against unauthorized access, modification, or deletion.			
Reference			
8500.02 Information Assurance Implementation, February 6, 2003, Page 60			
Q&A			
Q: How do I protect audit trails? **A:** *Reference ECRR: Event logs will be stored under C:/Windows/System32/Winevt/Logs. Folder permissions should be restricted to Administrators and System.*			

Table 2.1.9: ECVP-1 Virus Protection

Number	Name	Subject Area	Impact Code
ECVP-1	Virus Protection	Enclave Computing Environment	High
Implementation Guidance			
1. Protect workstations against malicious logic and keep current anti-virus signature files. 2. Update anti-virus signature files automatically.			
Reference			
Q&A			
Q: My company installs virus protection software such as McAfee or Symantec. Is this sufficient? **A:** *Yes, providing that anti-virus signature files are updated automatically.*			

Table 2.1.11: PECS-1 Clearing and Sanitizing

Number	Name	Subject Area	Impact Code
PECS-1	Clearing and Sanitizing	Physical Environment	High
Implementation Guidance			
1. Clear and sanitize all ERPToolsX data before redistributing workstation to a different user, scheduled maintenance, or equipment turn-in.			
Reference			
Q&A			
Q: Prior to decommissioning a laptop or workstation containing ERPTools X data, should I clear and sanitize (reformat the hard drive) the hard drive and system memory? In addition, if an authorized user of the ERPTools X application resigns, should the administrator reformat or sanitize the hard drive and system memory prior to transferring the laptop/system over to another unauthorized ERPTools X user? **A:** *The answer is YES to both questions. All ERPTools X information should be deleted/cleared/formatted/sanitized*			

prior to disposing or transferring of a system.

Table 2.1.12: PEDI-1 Data Interception

Number	Name	Subject Area	Impact Code
PEDI-1	Data Interception	Physical Environment	High
Implementation Guidance			
1. For devices that display or output ERPToolsX information in human-readable form, position them to deter unauthorized individuals from reading the information.			
Reference			
Q&A			
Q: My company positions all printers, screens, and screens displaying ERPTools X information away from windows and areas where unauthorized individuals can view the information. Is this sufficient? **A:** *Yes. You are compliant if computer screens, printers, VTCs, and other devices that display or output ERPTools X information in human-readable form are positioned to deter unauthorized individuals from reading the information*			

Table 2.1.13: PEPF-1 Physical Protection of Facilities

Number	Name	Subject Area	Impact Code
PEPF-1	Physical Protection of Facilities	Physical Environment	High
Implementation Guidance			
1. In facilities housing workstations that process or display ERPToolsX information, control all physical access points during working hours and guard or lock access points during non-work hours.			
Reference			
Q&A			
Q: The information system I use to enter data into the ERPTools X application is only accessed by personnel who have an ERPTools X account and have a valid need-to-know. Does this meet the requirement? **A:** *Yes. If only authorized account holders have access to the system, then the data is protected based on need-to-know; in doing so, you have met the requirement.* **Q: All facilities where ERPTools X information is stored have locked and/or guarded doors during non-working hours. Is this sufficient?** **A:** *Yes. As long as all physical access points (i.e. doors, windows, etc.) are locked or guarded during non-working hours, you have met the requirement.*			

Table 2.1.14: PESL-1 Screen Lock

Number	Name	Subject Area	Impact Code
PESL-1	Screen Lock	Physical Environment	Medium
Implementation Guidance			
1. Ensure workstation screen-lock functionality is enabled.			

2. When activated, the screen-lock function totally hides what was previously visible on the screen.
3. Enable this capability either by explicit user action or a specified period of workstation inactivity (e.g., 15 minutes) in accordance with agency standard operating procedures.
4. Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator (password).
5. A screen lock function is not considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

Reference

Q&A

Q: My computer contains ERPTools X data but doesn't have "screen lock" enabled? What should I do?

A: *1.In Windows 7 and Vista, right-click the desktop, and then select Personalize. In earlier versions, right-click the desktop, and then select Properties.*

2. In Windows Vista, the Personalization window will be open. Select Screen Saver.

In Windows XP, the Display Properties window will be open. Select the Screen Saver tab.

3. From the drop-down list, select a screen saver file.

4. In the "Wait:" field, set the amount of time you want the screen saver to wait for activity before starting (15 minutes is the AF required limit).

5. Depending on your version of Windows, check the appropriate box:

◦ *On resume, display logon screen*

◦ *On resume, password protect*

◦ *Password protected*

Click OK.

From now on, when the screen saver comes on, your workstation will be locked.

Table 2.1.15: PESP-1 Workplace Security Procedures

Number	Name	Subject Area	Impact Code
PESP-1	Workplace Security Procedures	Physical Environment	Medium

Implementation Guidance

1. The contractor and/or EPRToolsX users are responsible for ensuring an effective workplace security process is in place.

Reference

Q&A

Q: Company A makes sure their computers storing ERPTools X information, printed ERPTools X printed documents or backups stored onsite are secured during non-business hours. Is Company A compliant?

A: *Yes. As long as the ERPTools X computers, documents and backups are secure after hours, Company A is*

compliant.

Table 2.1.16: PESS-1 Storage

Number	Name	Subject Area	Impact Code
PESS-1	Storage	Physical Environment	High
Implementation Procedures			
1. Store ERPToolsX documents and storage media in a secure environment.			
Reference			
Q&A			
Q: Company A has ERPTools X information on laptops/documents. How can Company A become compliant with IA Control PESS-1 without locking all media and laptops in a safe? **A:** *When not using media, laptops, or documents containing ERPTools X information, place the media, laptops, or documents in a lockable office drawer, cabinet, or office space. Following these simple steps will make you compliant.*			

Table 2.1.17: PEVC-1 Visitor Control to Computing Facilities

Number	Name	Subject Area	Impact Code
PEVC-1	Visitor Control to Computing Facilities	Physical Environment	High
Implementation Guidance			
1. Ensure a procedure is in place for controlling visitor access.			
Reference			
Q&A			
Q: Company B controls who gets access to the facility hosting ERPTools X systems during working hours and ensures the facility is locked or guarded during non-working hours. Is Company B compliant? **A:** *Yes. Company B controls and monitors who visits the facility where ERPTools X systems and data is stored.*			

Table 2.1.18: PRRB-1 Security Rules of Behavior or Acceptable Use Policy

Number	Name	Subject Area	Impact Code
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	Personnel	High
Implementation Guidance			
1. All users read and sign Security Rules of Behavior.			
Reference			
Q&A			
Q: All users who have an ERPTools X account were required to sign the Security Rules and Behavior and provide a copy to the ERPIMS Program Manager.			

A: *ERPTools X users are required to sign the ERPIMS User Rules of Behavior Acknowledgement Form prior to an account being created and enabled. All ERPTools X contractors should be compliant with this control. If not compliant, please contact the ERPIMS Program Manager and request a copy of the form, sign the acknowledgment signature block, and return to the Program Manager.*

Table 2.1.19: PRTN-1 Information Assurance Training

Number	Name	Subject Area	Impact Code
PRTN-1	Information Assurance Training	Personnel	High
Implementation Guidance			
1. All ERPToolsX users comply with required IA training.			
Reference			
Q&A			
Q: Are ERPTools X users required to complete Information Assurance Awareness training? **A:** *Yes. ERPIMS .com customers are each required to provide initial Information Assurance Awareness Training (IAAT) Certificate along with the DD2875 when requesting access to the ERPIMS system. Records are reviewed and customers are notified by the ERPIMS support team when annual refresher training is required. Accounts are locked if training date exceeds 365 days. After 30 days, account is deleted.*			

Table 2.1.20: VIIR-1 Vulnerability and Incident Management

Number	Name	Subject Area	Impact Code
VIIR-1	Vulnerability and Incident Management	Vulnerability and Incident Management	High
Implementation Guidance			
1. Ensure a notification procedure is in place in case ERPToolsX data is either lost and/or compromised. 2. Notify the AFCEE IT Help Desk at, 210-395-8171 or via email at afceeitc@us.af.mil			
Reference			
Q&A			
Q: If ERPTools X data is either lost and/or compromised, what should I do? **A:** *Immediately notify the AFCEE IT Help Desk at, 210-395-8171 or via email at afceeitc@us.af.mil*			

APPENDIX A: LIST OF ACRONYMS AND ABBREVIATIONS

Acronym	Definition
AF	Air Force
AFCEE	Air Force Center for Engineering and the Environment
DIACAP	Defense Information Assurance Certification & Accreditation Program
DoD	Department of Defense
DoDI	Department of Defense Instruction
ERPIMS	Environmental Resources Program Information Management System
FOUO	For Official Use Only
IA	Information Assurance
MAC	Mission Assurance Category