

Live Training Transformation (LT2) Portal Security Policy

Prepared by:

US Army Project Executive Office for
Simulation, Training, and Instrumentation (PEO STRI)
12350 Research Parkway
Orlando, FL 32826-3275

9 August 2007

Table of Contents

| | |
|---|-----------|
| I. GENERAL INFORMATION | 4 |
| 1.0. INTRODUCTION | 4 |
| 1.1. OVERVIEW | 4 |
| 1.1.1. System Description..... | 4 |
| 1.1.2. Information Sensitivity..... | 4 |
| 1.1.3. LT2 Portal Management..... | 4 |
| 1.1.4. LT2 Portal Access..... | 5 |
| 1.2. PURPOSE | 5 |
| 1.3. SCOPE | 5 |
| 1.4. ORGANIZATION | 5 |
| 1.5. IMPLEMENTATION AND MANAGEMENT RESPONSIBILITIES | 5 |
| II. SECURITY POLICIES | 6 |
| 1.0. ACCESS CONTROL | 6 |
| 2.0. USER ID AND PASSWORD CONTROLS | 7 |
| 3.0. SESSION CONTROLS | 8 |
| 4.0. PHYSICAL PROTECTION OF IT RESOURCES | 9 |
| 5.0. FILE ACCESS CONTROLS AND PRIVILEGES | 9 |
| 6.0. NETWORK SERVICES | 10 |
| 7.0. INTERNET ACCESS | 10 |
| 8.0. AUDIT | 10 |
| 9.0. CONFIGURATION MANAGEMENT | 11 |
| 10.0. SOFTWARE INSTALLATION AND USAGE | 11 |
| 11.0. RISK ASSESSMENT | 12 |
| 12.0. VIRUS PROTECTION | 12 |
| 13.0. SYSTEM MAINTENANCE | 13 |

| | |
|---|-----------|
| 14.0. REMOTE ACCESS | 13 |
| 15.0. BACKUP & RECOVERY | 14 |
| 16.0. SECURITY VIOLATION DISCIPLINARY POLICY | 14 |
| 17.0. INFORMATION SECURITY AWARENESS TRAINING POLICY | 14 |
| 18.0. INCIDENT RESPONSE POLICY..... | 15 |

I. General Information

1.0. INTRODUCTION

1.1. Overview

1.1.1. System Description

The LT2 Portal was created to serve as a web-enabled interface into the assets and supporting tools of the LT2 Product Line. The LT2 Portal is a web-enabled interface that provides general information about LT2, the LT2 PLAF, and LT2 components.

The LT2 Portal contains all released LT2 work assets:

- Components submitted to LT2 for inclusion into the repository
 - Hardware Specifications
 - Interface Definition Documents
 - Software (libraries, executables, source code)
- Component Agreements
- Tools used to develop LT2 products
- Tools used to test and certify products submitted to LT2 for inclusion as a “Common Component”

The portal also contains the following documents and functionality:

- LT2 and CTIA documentation
- LT2 Help Desk
- LT2 FAQ
- Developer Docs
- Link to Bugzilla page
- Link to CTIA Help Desk
- Links to other LT2 Programs

The LT2 portal is intended to be the LT2 developer’s “one stop” shopping area for obtaining LT2 products, documentation, and related links.

1.1.2. Information Sensitivity

The information contained in the LT2 Portal is designated as Unclassified, Sensitive information, which is not releasable to the public.

1.1.3. LT2 Portal Management

The LT2 Portal will be configuration managed by the LT2 Portal Configuration Manager. This responsibility includes: authorizing the inclusion of new content, the modification of existing content, and the removal of obsolete content. Version control is critical as it is expected that multiple versions of many components will be in active use simultaneously. Equally as critical is the ability to track which components and versions have been used in which LT2 products.

1.1.4. LT2 Portal Access

Only authorized government and contractor personnel who are supporting the LT2 Product Line programs shall be permitted access to the LT2 Portal. The LT2 Portal is a PEO STRI website accessible through a web browser interface over a widely distributed network (e.g., the open internet using HTTP over secure socket layer, HTTPS). A login page, requiring authentication with a LT2 Portal authorized User ID and password, will be used to grant access into the LT2 Portal. Once past the login page, each user will have access to LT2 Portal content based on their assigned privileges and authorities (roles).

1.2. Purpose

This document establishes the security policies for operation of the LT2 Portal. The LT2 Portal shall be configured in accordance with this security policy to ensure traceability of responsibility for importing or exporting content and to ensure the confidentiality, integrity, and availability of that content.

1.3. Scope

The scope of this policy includes all personnel who have, or are responsible for an account (or any form of access that supports or requires a password) for the LT2 Portal, which is housed in the Integrated Development Environment (IDE) in Orlando, Florida.

1.4. Organization

This document is organized as a comprehensive collection of security policies, which together support the information assurance of the LT2 Portal. The security policies are contained in Section II of this document.

1.5. Implementation and Management Responsibilities

The LT2 Portal Security policy shall be implemented by applying industry and government standard information security concepts and techniques.

1. The LT2 Security Architect is responsible for the development and ongoing maintenance of the LT2 Portal Security Policy.
2. The LT2 government program manager shall be responsible for designating one or more Information Assurance Security Officer(s) (IASO) to oversee the implementation of the LT2 Portal security policy.
3. The LT2 Portal Site Manager is responsible for administration of the LT2 Portal, the LT2 Portal Security Procedures, and maintenance of User ID and password files.

II. Security Policies

1.0. ACCESS CONTROL

1. Access to the LT2 Portal will not be granted until the account registration is completed and submitted for approval, and approved by the LT2 Portal sponsor. A secret or interim secret clearance is required in order to obtain access to the LT2 Portal.
2. The LT2 Portal home page will contain a link to access the user registration page.
3. Required information, that must be filled in on the user registration page, before it may be submitted, is as follows:
 - a. First Name
 - b. Last Name
 - c. Email Address
 - d. Type of access the user is requesting (Document Only or Document and Source Code Access)
 - e. Program with which the user is associated and for which the user is requesting a LT2 Portal Account
 - f. Organization
 - i. If Government employee: Specify affiliated government organization.
 - ii. If contractor employee: Specify Company by which employed.
 - g. Office Phone
 - h. Annotate that the user has read and accepted, the LT2 Portal Security Policy.

Note: User's that do not accept the LT2 Portal Security Policy will not be allowed to proceed with the account request process or granted access.
4. Other information fields may be added to the registration page; however, they would not be required fields.
5. After receiving a completed registration form, the system will send an e-mail to the LT2 portal Administrator. The LT2 Portal administrator will grant or deny access to the Portal.
6. The LT2 portal Administrator will review the registration request for access and either grant or deny access.
 - a. Upon account approval, the system will automatically send an e-mail notification of approval to the user, which will include a one-time password to be used for the first login to the LT2 Portal. The one-time password shall be changed after first login.

- b. LT2 Portal users may either request Document Only or Document and Source Code access. Users requesting access to Source Code must also submit a completed LT2 Distribution Agreement to the LT2 Portal administrator. The Administrator validates information on the request before granting that access level or role to the user.
 - c. A secret or interim secret clearance is required in order to obtain access to the LT2 Portal.
 - d. If the Portal Administrator denies access to the user, the system will automatically send an e-mail notification to the requesting user, denying access to the portal.
 - e. Once an account is granted to a user, that user will be assigned a username. The username is generally first initial, and lastname. In the case where this combination is already in use, an increasing digit will be appended until a unique username is generated.
7. The user's User ID, Password, and access rights data will be stored and maintained in the system.
 8. The LT2 Portal Administrator is the only person who can change, add, or delete roles or their associated permissions.

2.0. USER ID AND PASSWORD CONTROLS

1. All users must have registered to establish a User ID and Password for access to the LT2 Portal. Registration will be in accordance with (IAW) Section II, paragraph 1.0 of this document.
2. All LT2 Portal user accounts will be re-validated semiannually with the LT2 Portal Administrator to ensure there have been no changes in personnel status.
3. Each LT2 Portal user will be issued a unique account name/user id IAW Section II, paragraph 1.0 of this document.
4. Each account will have a valid password and be assigned to a person with primary responsibility, or the account will be disabled.
5. Passwords will be a minimum of **ten** alphanumeric characters in length and will be a mix of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each of the four types of characters (for example, x\$T!oTBn2!) and can be user generated .
6. Passwords will not contain social security numbers (SSNs), birthdays, UserIDs, telephone numbers, names, slang, military acronyms, call signs, dictionary words, more than two (2) consecutive or repetitive characters, system identification, or name, or be easy to guess (e.g., mypassword, or abcde12345).
7. Passwords shall not be displayed when input, and users shall be attentive to persons attempting to view their password while being entered.
8. Individual User passwords shall not be shared with anyone.

9. Authentication data (passwords) shall be stored in an encrypted form. When technically feasible, they will be stored in files not readable by world/everyone.
10. Storage of a password in clear-text form will only be permitted when absolutely necessary and under acceptable risk circumstances. All such cases require justification in writing with IASO approval.
11. All user-level passwords for access to the LT2 Portal must be changed at least every **90** days.
12. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every **90** days, or anytime an administrator with knowledge of the privileged password is reassigned.
13. The number of people who have knowledge of the passwords to privileged accounts (system and application) will be strictly limited and documented.
14. Shared or Group accounts will not be used.
15. Users shall be required to login with their uniquely assigned User ID and password each time they access the LT2 Portal.
16. When available, systems will be configured to require a password for access to single-user or setup mode.
17. Default passwords to pre-installed vendor accounts shall be changed upon installation or upgrade of a software package.
18. On Unix systems, direct logins to the root account will be limited to the console.

3.0. SESSION CONTROLS

1. The following notice and consent banner will be included on all DoD Web sites, with security and access controls. It will be part of the log-on screen.

ATTENTION

“This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be

- used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.”
2. Systems will be configured to deter unauthorized access attempts. After 3 consecutive failed logons to an account, the account will be locked until reset by a LT2 Portal administrator.
 - a. Within 72 hours of any user lockout, the appropriate IA personnel will verify the reason for failure; and the LT2 Portal administrator will maintain a written record of all reasons for failure for 2 years.
 - b. Only the LT2 Portal administrator can reinstate a locked out user. This will be done only after the reason for the failed logons has been determined.
 3. Unless required for unattended processing, users will log out when finished with their session, or at the end of the workday.
 4. Users will use a password enabled terminal locking or screen saver utility when leaving their terminal or workstation unattended.
 5. Screen savers will be configured to automatically engage after 10 minutes of inactivity.

4.0. PHYSICAL PROTECTION OF IT RESOURCES

1. All LT2 Portal Servers, Network devices (e.g. routers, switches), and backup media will be physically located within a controlled access area to preclude theft, vandalism, or access by non-authorized persons.
2. Controlled access areas include areas secured with key locks, cipher locks, card readers, biometric devices, or other similar mechanisms.

5.0. FILE ACCESS CONTROLS AND PRIVILEGES

1. File accesses and privileges will be established on the basis of least privilege and need-to-know.
 2. System files and directories will be owned by a privileged account and belong to a privileged group.
 3. System files and directories will not be writeable by non-privileged accounts.
 4. The use of world writeable directories will be minimized.
 5. Permissions on world writeable directories shall be set to permit deletion of files only by the owner.
 6. Files containing security relevant information (e.g. audit, authentication data, security configuration data) shall not be readable by non-privileged accounts. Any exceptions shall have a documented justification with approval by the LT2 Portal IASO.
 7. The LT2 Portal software configuration managed repository will be configured to limit write access to only those personnel specified in the LT2 Portal User Access Document.
-

8. Each group identifier shall be documented to include its purpose, access privileges, and requirements for membership.

6.0. NETWORK SERVICES

1. All enabled network services will be documented and approved by the LT2 Portal IASO.
2. Network services available on LT2 Portal servers will be limited to those required to support LT2 Portal authorized user and administrative activities.
3. Services with known security vulnerabilities shall be disabled unless absolutely necessary for the LT2 Portal to function correctly.

7.0. INTERNET ACCESS

Internet access to the LT2 Portal is the primary means of connection for authorized users. Users obtain authorization to access the LT2 Portal via the Registration Process described in Section II, paragraph 1.0 of this document.

8.0. AUDIT

1. Auditing will be configured and implemented on all LT2 Portal servers. Any exceptions shall have a documented justification with approval by the LT2 Portal IASO. The audit trail will document the following:
 - a. The identity of each person and/or devices accessing the LT2 Portal
 - b. The date and time of the access including:
 - i. Logon (unsuccessful and successful) and logout (successful)
 - ii. User lockout due to three failed user log-on attempts
 - iii. Administrative Actions and use of privileges (unsuccessful and successful)
 - c. User activities sufficient to ensure user actions are controlled and open to scrutiny.
 - d. Activities that might modify, bypass, or negate safeguards controlled by the LT2 Portal.
 - e. Security-relevant actions associated with periods of processing or changing of security levels or access privileges.
 2. A configuration baseline of all system and security relevant files will be maintained for each LT2 Portal server.
 3. All audit files and directories will be readable only by personnel authorized by the IASO.
 4. Audit files will be retained at least one year.
 5. On a weekly basis, the IASO or designee will review the audit trails and/or system logs for the following:
 - a. Excessive logon attempt failures by single or multiple users
 - b. Logons at unusual/non-duty hours
-

- c. Unusual or unauthorized activity by LT2 Portal Administrators
- d. Unusual or suspicious patterns of activity

9.0. CONFIGURATION MANAGEMENT

1. LT2 Portal content is configuration managed IAW the process defined in the LT2 Portal Rules and Guidelines.
2. At a minimum the configuration management plan and process defined in the LT2 Portal Rules and Guidelines will:
 - a. Use a source code Configuration Management (CM) system.
 - b. Describe how the CM system is used.
 - c. Describe the method used to uniquely identify each configuration item.
 - d. Describe how to determine which configuration items comprise the LT2 Portal software baseline.
 - e. Describe the mechanisms to be used to ensure that only authorized changes are made to the configuration items.
 - f. Provide mechanisms to record evidence of what changes have been made to configuration items, including when and who made the change.

10.0. SOFTWARE INSTALLATION AND USAGE

1. Adherence to applicable software licenses is required.
2. Use of “shareware” or “freeware” is prohibited unless specifically approved through IA personnel. Shareware/Freeware must have a documented justification and approval by the IASO. Shareware/Freeware is defined in this context as source code or binary code that is downloaded from the Internet that:
 - a. Has no clearly defined provider channel
 - b. Has no clearly defined support path, or
 - c. Has no chain of responsibility for updates and security notification
3. Use of “open source” software (for example, Red Hat Linux) is permitted when the source code is available for examination of malicious content, applicable configuration implementation guidance is available and implemented, a protection profile is in existence, or a risk and vulnerability assessment has been conducted with mitigation strategies implemented with DAA and CCB approval. Open Source is defined in this context as software where the source code, i.e., code that is in human readable rather than machine-readable form, is publicly available for anyone to modify or redistribute.
4. All system software shall be documented to include the corresponding provider and version number. The ability to generate a software report upon request will satisfy this documentation requirement.
5. Only authorized LT2 Portal system or network administrators are authorized to install software.

11.0. RISK ASSESSMENT

1. Periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation will be conducted. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.
2. The execution, development and implementation of remediation programs are the joint responsibility of the IASO and the organization responsible for the system's area being assessed. Users are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Users are further expected to work with the IASO led Risk Assessment Team in the development of a remediation plan.
3. At a minimum, the IASO or designee shall monitor the following security alert bulletins:
 - a. System Administration, Networking and Security (SANS) www.sans.org
 - b. Federal Computer Incident Response Capability (FedCIRC) www.fedcirc.llnl.gov
 - c. Computer Emergency Response Team (CERT) www.cert.org/pub/alerts.html
4. Quarterly, the IASO and IT staff shall review all applicable security bulletins/patches to determine if the security bulletin is relevant (vulnerability is likely to be exploited) in the LT2 Portal environment. The IT staff shall install security patches determined to be relevant. Note: *The IASO may call for an immediate review of certain security bulletins that are of a high-risk nature.*

12.0. VIRUS PROTECTION

1. All DOS/Windows and Macintosh based systems shall have PEO STRI standard, supported anti-virus software installed and configured to automatically screen for viruses. Note: *The PEO STRI anti-virus software is available from the PEO STRI IAPM.*
 2. At a minimum, the virus signature files for anti-virus software shall be updated twice per month.
 3. When a virus is detected, users will:
 - a. Save all files and turn off their computer.
 - b. Contact a LT2 Portal administrator
 - c. Cooperate and provide information regarding the circumstances of the virus infection.
 - d. Quarantine the affected computer and any removable media (floppy disks, zip drives, CDs etc.) that may be infected until the computer has been cleaned of all viruses.
 4. Recommended processes to prevent virus problems:
-

- a. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- b. Delete spam, chain, and other junk email without forwarding.
- c. Never download files from unknown or suspicious sources.
- d. Avoid direct disk sharing with read/write access unless there is absolutely a requirement to do so
- e. Always scan a disk from an unknown source for viruses before using it.
- f. Back-up critical data and system configurations on a regular basis and store the data in a safe place

13.0. SYSTEM MAINTENANCE

1. Only trained and knowledgeable LT2 Portal system or network personnel will perform modifications to system hardware or software.
2. Records will be maintained for all major activities related to system maintenance (hardware and software).
3. Outside vendor maintenance personnel will not be given access to privileged accounts unless a LT2 Portal system or network administrator monitors their activities.

14.0. REMOTE ACCESS

1. It is the responsibility of the LT2 Portal to ensure that their remote access connection is given the same consideration as the user's on-site connection. At a minimum, the remote devices will be protected consistent with access to Sensitive But Unclassified information.
2. Contractor or government agencies with remote access privileges will implement physical safeguards to ensure only authorized persons use remote access equipment.
3. Remote access must be strictly controlled, and positively identify and authenticate all users before granting access. Control, identification and authentication will be enforced via the Access Control Policy and User ID and Password Control Policy in paragraphs 1.0 and 2.0 respectively of this document.
4. Remote device password save-function will be disabled to prevent storage of plain text passwords.
5. Remote dial-in access will not be allowed to individual workstations.
6. The LT2 Portal will employ host assessment software tools, firewalls, and intrusion detection systems to detect unauthorized access and to prevent exploitation of network services.
7. The LT2 Portal will employ a "Time-Out" protection feature that automatically disconnects the remote device after 10 minutes of inactivity.

8. Passwords will be encrypted as they transverse the network.
Note: NSA hardware encryption is the preferred policy, unless the respective activity obtains a waiver from DISC4. DISC4 will consider Kerberos and/or Secure Shell (SSH) as waiver candidates/temporary alternatives to hardware encryption for the protection of unclassified identification and authentication information.

15.0. BACKUP & RECOVERY

1. Copies of the LT2 Portal files shall be maintained on a server that has scheduled backups.
2. LT2 Portal servers will be backed up on a regular schedule (e.g. incremental and/or full backups) to ensure that in the event of a failure, systems may be restored with data that is not older than 24-hours.
3. Backup media will be appropriately labeled to facilitate system restoration.
4. Backup media stored onsite will be physically located within a controlled access area to preclude theft, vandalism, or access by non-authorized persons.
5. LT2 Portal backup media will be rotated offsite, to a location at least one mile away, on a schedule to ensure that in the event of a local facility catastrophe, systems may be restored with data that is not older than one week.

16.0. SECURITY VIOLATION DISCIPLINARY POLICY

1. In general, the LT2 Portal disciplinary policy regarding security violations shall be in accordance with the applicable contractor or government site policy.
2. At minimum, all violations of the LT2 Portal security policy shall be documented in writing and reported to the appropriate Contractor or Government Security Organization and Program Manager.
3. LT2 Portal System and Network Administrators have the authority to immediately terminate a user's access if they become aware of malicious activities that may result in harm to LT2 Portal IT resources. Immediately upon this type of action, the LT2 Portal System or Network Administrator will notify the appropriate Contractor or Government Security Organization and Program Manager of their action to terminate the user's access.

17.0. INFORMATION SECURITY AWARENESS TRAINING POLICY

1. Before being granted access to the LT2 Portal, each LT2 Portal user shall read and accept the LT2 Portal Security Policy, which will constitute initial security awareness training. The acceptance of the LT2 Portal Security Policy will be indicated on the registration page.
2. If the LT2 Portal user does not accept the LT2 Portal Security Policy, the LT2Portal will not allow registration to continue. A registration request will not be submitted without a LT2 Portal user accepting the LT2 Portal Security Policy.

3. Authorized users must review the LT2 Portal Security Policy on an annual basis.
4. In addition to the above, an Information Assurance awareness training program shall be established IAW paragraph 4-3 a. (8) of AR 25-2.

18.0. INCIDENT RESPONSE POLICY

1. Security incidents will be investigated to determine their cause and the cost effective actions required to prevent reoccurrence.
2. If the cause of an incident can be directly attributed to administrative error and be readily corrected then no further action is required.
3. Suspected or actual incidents, not attributable to administrative error, will be reported immediately to the LT2 Portal IASO, who will notify the appropriate Information Assurance Manager (IAM). Concurrently, the operator and IASO will notify the PEO STRI Information Assurance Program Manager (IAPM).
4. After initial notification, a brief written statement containing the location affected, system, a description of the suspected or confirmed incident, action taken, and point of contact will be provided to the PEO STRI IAPM within six hours of incidence occurrence.
5. The PEO STRI IAPM will make the decision to notify or not notify the Army Computer Response Team/Coordination Center (ACERT) or its subordinate CERT infrastructure and request immediate technical assistance.

Examples of the types of incidents that will be reported include, but are not limited to, the following:

(1) Known or suspected intrusions or attempted intrusions into classified and unclassified AIS by unauthorized users or by authorized users attempting unauthorized access.

(2) Unauthorized access to data, files, or menus by otherwise authorized users.

(3) Indications of an unauthorized user attempting to access the AIS, including unexplained attempts to log-on unsuccessfully from a remote terminal.

(4) Indications of unexplained modifications of files or unrequested “writes” to media.

(5) Unexplained output received at a terminal, such as receipt of unrequested information.

(6) Inconsistent or incomplete security markings on output with extraneous data included in the output, or failure to protect the output properly.

(7) Abnormal system response.

(8) Malicious software.

(9) Alerts by network intrusion detection (NID) systems installed to detect “hackers” and other unauthorized personnel attempting system penetrations.

6. The LT2 Portal IASO will review all incident reports and related documentation and, in cooperation with other security and investigative personnel, advise the appropriate IAM and commander, or manager having jurisdiction over the possible system penetration or security violation. The IAM will ensure that all available audit trail information is maintained until the incident is resolved.
7. In those cases where AIS security incidents affect the supported user community, the IAM must formally advise all users of the problem and the action taken or expected. The centralized incident reporting activity for the Army will, through the IAM or IASO, as appropriate, provide the user with guidance and instructions received from the Criminal Investigation Division (CID) or Counterintelligence (CI).