U.S. Department of Justice
Federal Bureau of Prisons

P R O G R A M S T A T E M E N T
OPI: IEV/MIS
NUMBER: 8051.04
DATE: March 18, 2015

UNICOR Information Technology Systems Administration

/s/
Approved: Charles E. Samuels, Jr.
Director, Federal Bureau of Prisons

1. PURPOSE AND SCOPE

To define standards for the management of UNICOR (Federal Prison Industries) Information Technology (IT) systems and resources and their administration.

This Program Statement establishes standards that govern the life cycle management of UNICOR IT hardware and software systems and defines procedures for effective management of IT resources. It provides a mechanism for rapidly incorporating new IT standards established by the Department of Justice or higher-level Federal IT regulatory authority.

With the exception of security oversight and vulnerability management by the Chief Information Security Officer (ISO), this standard does not apply to UNICOR "Production" systems. UNICOR Production systems include any hardware, software, or combination thereof used for task-specific purposes. Production systems include any hardware or software configured and used specifically to satisfy the requirements of a UNICOR contract or those systems required by a UNICOR customer for the production of goods or services under a contract.

a. Summary of Changes

Policy Rescinded
P8051.03 UNICOR Information Systems Administration (9/25/2003)

- Incorporates new Technical Reference Guides (posted on www.FPI.gov) that govern IT Management processes and procedures in specific areas.

b. **Program Objectives.** Expected results of this program are:

- Software and data stored on UNICOR computer systems will be properly safeguarded.
- UNICOR computer resources will be effectively managed and protected from environmental damage and unauthorized access.
- UNICOR System Administrators (SA) will be adequately trained to support the UNICOR Information Technology Network and provide technical assistance to UNICOR staff.

c. **Institution Supplement**. None required. Should local facilities make any changes outside the required changes in the national policy or establish any additional local procedures to implement the national policy, the local Union may invoke to negotiate procedures or appropriate arrangements.

2. ROUTINE PROCEDURES

To ensure UNICOR IT systems and data are protected, the Management Information Systems Branch (MISB) has identified standard controls and corresponding operational and configuration standards.

a. **UNICOR IT Standard Controls** define requirements that apply to all data centers, systems, staff, or resources throughout UNICOR. These include:

- Account Management.
- Data Management.
- Change Management.
- Environmental Controls.
- Vulnerability Management.

b. **MISB Operational and Configuration Standards** are Technical Reference Guides that define specific system configuration procedures, system specifications, or standards that govern IT resource management practices to which Systems Administrators (SA) must conform. Technical reference documents may apply to MISB as a whole or only to specific practices of different elements (Sections) within MISB. MISB standards include:

- SAP Standard Operating Procedure.
- Applications Development Standards.

- Field Procedures and Systems Standards.
- E-Commerce Electronic Data Interface Standards.
- ISM Operating Procedures and Configuration Standards.

UNICOR Standard Controls and MISB Technical Reference Guides ensure:
- Access to UNICOR systems is controlled and documented.
- Systems are configured correctly.
- Security systems/protections are implemented properly.
- Systems are maintained correctly so that daily operations are not adversely affected.
- Data accuracy and accessibility is ensured.
- System performance is routinely monitored and reported.

Performance of those tasks ensures that:

- Critical data is properly backed up.
- System logs are reviewed for any abnormal events and resolved.
- Users are prevented from accessing restricted resources or sensitive data.
- The current system is performing optimally.

3. INFORMATION TECHNOLOGY GENERAL CONTROLS

UNICOR systems and business data integrity must be protected at all times. Critical systems must be properly secured in locations that address environmental issues, such as power and ventilation, fire prevention, and disaster recovery.

a. **Computer Room and Data Closet Access**. Each computer room and data closet must have a secure lock on the door; access is restricted to authorized staff. An Entry Authority List (EAL) is posted at the entrance to these spaces. Under no circumstances may doors to these spaces be left open unattended.

b. **Environmental Conditions.** Environmental conditions must be monitored to prevent damage. Each location or data center ensures that environmental control equipment is installed to maintain industry-recommended temperatures and relative humidity.

c. **Computer Room Construction.** The Program Statements **Design and Construction Procedures** and **Factory Construction/Activation Manual – FPI** contain detailed specifications for new computer room construction. Staff at existing institutions ensure new computer rooms comply with these standards.

d. **Data Management.** System backups are performed frequently. Backup media are stored in fireproof containers or at offsite secure locations. Systems Administrators must be familiar with backup software and procedures used to restore data.

e. **Systems and Software Maintenance**. Hardware, operating system, and application updates are applied in a timely manner. Operating system and application patches are tested and documented using non-critical or non-production systems before being applied to any production system.

f. **Access Control**. Access control procedures protect UNICOR systems from unauthorized physical and logical access. They ensure or validate that a system user has received proper clearance and has supervisory approval before access, and that control measures are documented. Access control procedures apply to any means of access to UNICOR systems and to any system owned by UNICOR.

g. **System Refresh**. MISB establishes a Hardware /Software Refresh Cycle to distribute the costs of replacing aging hardware/software over several years. Funding is requested in each Fiscal Year cycle, subject to the approval of corporate management or the Board of Directors.

h. **System Development Life Cycle (SLDC)/Change Control**. UNICOR complies with SDLC and Change Control policies defined by the Department of Justice.

i. **Audit/Program Review.** MISB ensures applicable general control and Information Technology Systems Standards (ITSS) security standards are followed through periodic internal reviews.

j. **Systems Administrators (Field and Central Office)**. MISB directs System Administrators providing IT support at factory locations and in the Central Office. MISB SAs also participate in temporary duty assignments away from their primary support locations in direct support of UNICOR operations. The UNICOR SA serves as the Information Security Officer (ISO) for UNICOR factories they support. Their security responsibilities are defined by the Department of Justice to the extent they do not violate segregation of duty policies. The UNICOR Chief ISO in the Central Office has overall security oversight within UNICOR, as delegated by the CIO.

4. DOCUMENTS MANAGEMENT

UNICOR IT Standard Controls and MISB Technical Reference Guides are posted on www.FPI.gov unless they contain sensitive information. MISB designates a Documents Manager

to maintain standards and guides. MISB Section Chiefs annually review standards and guides to ensure they remain current.

Printed copies may be maintained but must be protected from unauthorized staff or inmate access.

MISB updates Technical Reference Guides to address improvements in technology and procedures. SAs are notified via e-mail when updates are made.

5. **TRAINING**

MISB staff are provided training opportunities to the fullest extent possible. Technological requirements, policy, or security mandates are the basis for providing training. The needs of the organization and the employee's ability to perform his/her duties are considered when determining whether training should be provided.

MISB conferences are held every three years (or as approved by the Assistant Director, Industries, Education, and Vocational Training Division). They provide MISB staff a collective training opportunity and allow sharing of expertise among sections.

All staff must complete the Annual Needs Assessment survey. Staff may request training offered by the agency or by local colleges, technical schools, or commercial vendors. Training is approved by direct supervisors, who ensure requests are cost-effective and beneficial to the agency.

6. **ASSISTANCE**

Direct questions to the Chief Information Officer, UNICOR Management Information Systems Branch.

7. **AGENCY ACA ACCREDITATION PROVISIONS**

- Standards for Adult Correctional Institutions 4th Edition: 4-4101.
- Performance-Based Standards for Adult Local Detention Facilities, 4th Edition: 4-ALDF-7D-22.
- Standards for Administration of Correctional Agencies, 2nd Edition: 2-CO-1F-06.

REFERENCES

Program Statements

P1237.13	Information Security Programs (3/31/06)
P4220.05	Design and Construction Procedures (2/15/00)
P8041.03	Factory Construction and Activation Manual – FPI (12/11/97)

Other References

NIST 800-53A	Information Resource Standards
DOJ-2640.2	Department of Justice Information System Security
FISMA	Federal Information Standards Management Act

Records Retention Requirements

Requirements and retention guidance for records and information that apply to this program are available in the Records and Information Disposition Schedule (RIDS) on Sallyport.