Information Technology Image Retention Policy

BALL STATE UNIVERSITY INFORMATION SECURITY SERVICES

1. Introduction

The law requires Ball State University to retain and maintain certain types of records, usually for a specified period of time. Failure to retain those records for the minimum period of time could subject the university to penalties and fines, cause the loss of rights, or seriously disadvantage the university in litigation. This policy outlines image retention at Ball State. All employees are expected to comply with image retention guidelines except for defined exceptions.

2. Scope

This policy addresses the retention of scanned images, specifically the requirements of Social Security Numbers in scanned documents and maintenance required in protecting the information. Violations of this policy are unethical and possibly unlawful and may result in sanctions as discussed below.

Long term policy for retention of scanned images

- **A.** General rule: All information scanned into the imaging system will be retained for a period of seven (7) years from the date the image is created, after which time the image will be securely destroyed.
- **B.** Exceptions for retention for longer than seven (7) years must be recommended by the Banner Implementation Leadership Team (ILT) and approved by the Executive Management Support Team (EMST) and the directory of university auditing. The ILT shall grant exceptions for the following reasons:
 - A legal requirement (statute, regulation, or agency regulation) (Example: Payroll Employee Benefits (PEB) and Human Resource (HR) files for pension and employment related documents.)
 - A relevant best practices standard as set forth by a professional body or organization (Example: American
 Association of Collegiate Registrars and Admissions Officers (AACRAO) suggestion for retention and disposal of
 student records).
 - **3.** A particular business case put forth by a department.

It is understood that in some cases, extensions for certain records falling into one or more of the above exceptions will require images be retained permanently. In each case where an exception is granted, the department responsible for information granted an exception must document and maintain the requirements of the accept standard; and work with the Banner Document Management Systems (BDMS) technical support team to implement the approved extension.

4. Policies related to Social Security Numbers (SSN) in scanned documents

- **A.** Any documents which are scanned into the new imaging system containing SSN information will be redacted, masked, or protected as follows:
 - **1. Redaction**: In the event there are <u>no</u> justified business cases where the full SSN must be maintained on the image, then at least the first six digits of the SSN must be permanently obscured through an approved reaction process which makes these digits permanently unreadable.
 - 2. Masking: In the event there are <u>some</u> justified business cases where the full SSN must be maintained on the images as well as other business cases where access to the full SSN is not justified then the SSN must be

- masked and appropriate permissions applied to the masking, such that those persons with a justified business case for seeing the full SSN can access it and those persons without such justified may see either none of the SSN, or if needed for identification purposes only the last four digits of the SSN.
- 3. Protected: In the effect <u>all</u> business uses of the document require the full SSN, and where no offices have access to the document who do not have a need to maintain the full SSN on the imaged document, then no masking or redaction of the SSN shall take place, and the instead the document shall be protected through appropriate permissions such that only those persons having established business case for access to the full SSN will have any access to the image.
- B. Unless approved as described below, any SSN must be redacted.
- C. In any of the above cases (masking, redaction, or protection) the full SSN may also be permitted as a search field only, meaning that the full SSN is maintained an index value associated with the image used to locate the document (such as by typing the SSN into a search field) but where this index value is not displayable, extractable, or otherwise accessible for any other purpose.
- D. Maintaining the full SSN in a readable format as part of the image (through masking or protection as described above) will be by exception and only when absolutely necessary as follows:
 - 1. Exceptions will require a showing of some particular requirement (statute, regulation, or agency requirement) for which redaction or masking of the SSN would be not possible.
 - Exceptions to this policy, and access controls for images of the full SSN will be tailored as narrowly as possible so that the full SSN is imaged and available only when required by statue, regulation, board resolution, or executive mandate.
 - 3. Exceptions to the above must be recommended by ILT and approved by EMST, the Director of University Auditing, and the Director of Information Security.

5. Policies related to maintenance of paper records that contain full (or partial) Social Security Numbers

- **A.** Documents that are not scanned into BDMS, or that are scanned and for which a paper copy is retained, are subject to this policy.
- **B.** Documents must be kept in a physical area with restricted access. The physical area must secure all files behind a locked door.
- **C.** Access to the physical area is limited to a narrowly defined list of persons whose role requires access to the records containing SSNs.
- D. The ILT and the Director of Information Security shall approve the list of roles that require access to the secured files.

6. ENTERPRISE RESOURCE PLANNING (ERP) RELATED POLICIES

A. Conversion of documents will follow the procedures above, and images exceeding the retention period outlined above will not be converted.

7. HISTORY

Approved by EMST and EC: 03/19/2012