

Chapter Name

4.0 INFORMATION MANAGEMENT

Chapter Number Title

4.10 End-User Reporting Control and Data Integrity

1.0 Purpose

The accuracy, integrity, confidentiality, and control of official University data are critical to the proper and lawful functions of Eastern Michigan University. EMU relies on desktop productivity tools and end-user reporting tools as an integral part of its reporting environment.

This policy ensures the use of these tools is subject to the appropriate types of control relative to the process's complexity or importance to University decision-making and legal requirements, as well as the confidentiality of the data being manipulated.

2.0 Scope

This policy applies to any person in possession of EMU data, who develops or maintains processes that utilize desktop productivity or reporting tools which manipulate data for any of the following reasons:

- management decision making
- transfer of information between systems
- legal compliance reporting

Processes used to track or log documents or work flow to support operational processes, such as a listing of open claims, unpaid invoices, or other information that previously would have been retained in paper file folders, would be rated as LOW in criticality or complexity, and policy dictated controls would not be necessary.

In comparison, enrollment statistics would be rated HIGH in criticality to University decision making, and therefore *would* require audit controls on data calculations, on the process environment, and on the authentication and actions of persons authorized to modify calculations (see 3.0 Policy below).

In cases where policies conflict with each other, the most restrictive rule will always apply, unless explicitly stated otherwise.

3.0 Policy

Where reporting processes fit the scope description above, each department creating processes utilizing EMU's desktop productivity or reporting tools will create and document the process environment, following the data processing principles below:

- 1) Maintain an inventory of each process that includes: name, brief description, creator, and department utilizing the process, change history, and complexity level.
- 2) Maintain current and accurate documentation of each process.
- 3) Guarantee that processes are backed up.

- 4) Guarantee that processes can be restored from a backup if restoration is necessary.
- 5) Implement appropriate security controls relative to the importance of the process to the University and your department.
- 6) Store and handle data in accordance with the Data Classification Policy [Information Technology (IT) Policy 7.2] and Electronic Data Storage and Transmission Policy (IT Policy 7.3).
- 7) Restrict modifications of the process to qualified staff.
- 8) Establish verification and certification procedures for the process.
- 9) Establish a process to reconcile the output to the original source.
- 10) Establish a distribution method to guarantee that the current version is being used at any time.
- 11) Guarantee that processes do not circumvent ERP Security

Departmental directories on the EMU shared drives are available for the implementation of this type of environment which provide scheduled backup and restore capabilities.

The Division of Information Technology (DoIT) is available to review a specific situation whenever there are questions, concerns or doubts, and to advise individual end-users and managers about potential risks.

4.0 Responsibility for Implementation

Departmental representatives will be designated by a Senior Administrator and their names provided to the Director of IT Security Administration.

5.0 Enforcement

Departmental representatives, with the assistance of the Director of IT Security Administration, will enforce this policy.

Any user having intentionally violated this policy is subject to loss of access to EMU's desktop productivity or reporting tools regardless of job responsibilities requirements. EMU disciplinary actions may result from unsatisfactory job performance.

Any employee found to violate federal or state of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including discharge.
- Criminal prosecution.

Any student found to violate federal or state of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU's Student Code of Conduct. Any suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including suspension or expulsion from school.
- Criminal prosecution.

If you break the law, you can be prosecuted. Even if you are not charged criminally, you can be held personally liable, and you can be suspended or dismissed from the University, or fired if you are an employee.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

6.0 Definitions	
<u>Term</u>	<u>Definition</u>
Desktop Productivity Tools	Vendor software requiring limited technical expertise used to perform calculations, analyze, track, or manage information. Examples are: Microsoft Access, Microsoft Excel, etc.
End-user Reporting Tools	Vendor software requiring limited technical expertise used to extract and format data from the ERP System for departmental use. Examples are: Microsoft Access, Crystal Reports, etc.
Complexity Levels	<p>LOW: Processes used as an electronic logging and information tracking system.</p> <p>MODERATE: Processes used to perform simple calculations such as using formulas to total certain fields or calculate new values. Processes used to translate or reformat information.</p> <p>HIGH: Processes used to support complex calculations utilizing macros or to link multiple tables together.</p>
Backup	The maintaining of multiple copies of the same process in different locations in case one is lost, deleted, corrupted or the original location becomes unavailable.
Restore	Process used to retrieve a file or process from a secondary or backup location.
Senior Administrator	As defined by the EMU Department of Human Resources at the relevant time.

7.0 Revision History			
<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Popp	Initial draft	April 25, 2006	
Policy Committee	Committee revisions	June 6, 21, 2006	
Policy Committee	Committee revisions	July 18, 2006	
Dorendorf	Functional Security Team Comments	March 12, 2007	
J. French	Edits	October 6, 2008	
A. Barr	Editing, rewording purpose 1.0; added catch-all in bulleted list in 2.0 Scope; substantial edit and expansion of 5.0 Enforcement to conform with the December 2008 Acceptable Use Policy . Submitted to Policy Committee for review at meeting on January 27, 2009; note to resolve policy number 4.1 or 4.10; sent to Legal for review.	January 23, 2008	
Policy Committee	Reviewed and agreed to changes. See next entry.	January 27, 2009	
A. Barr	Deletion of dragnet provision in Section 2.0 Scope, add definition for Senior Administrator; footer.	January 28, 2009	