

# Privacy of IT Collected Data

## Policy Information

### Issuing Office

Information Services

### Affected Parties

Students, Alumni, Faculty, Staff, Guests

### Policy Language

1. This standard applies to the extraction and use of data:

1.2 In support of corrective action for an employee;

1.3. For potential evidence of a violation of the acceptable use of Liberty University computing resources;

1.4. Requested by law enforcement agencies as evidence in a legal investigation.

1.5 This standard does not apply to IT collected data that is regularly reported on by Nicus.

2. Any discovery, extraction and use of data regarding individuals? consumption of IT services in support of corrective action for an employee will follow standard procedures for the collection and distribution of that data.

3. Any discovery, extraction and use of data that is deemed to be potential evidence of a violation of acceptable use of Liberty University computing resources will follow standard procedures for the collection and distribution of that data.

4. Any discovery, extraction and use of data requested by law enforcement agencies as evidence in a legal investigation will follow standard procedures for the collection and distribution of that data.

### Policy Rationale

This policy defines how data of a University employee's consumption of IT services that is collected by Information Technology and its associated software applications and not regularly reported on, can be extracted and distributed.

### Definition of Glossary Terms

None specified

## Procedural Information

### Procedures

1. Standard Operating Procedure

1.1 Requester submits request to VP of Human Resources

1.2 Requester submits request to CIO

1.3 If the VP of Human Resources or the CIO deny the request, the process ends

1.4 If the VP of Human Resources and the CIO approve the request, an IT employee collects the data

1.4.1. Once the data is collected, it is delivered to the Requestor

2. Requesting IT-Collected data

2.1. General guidelines.

2.1.1. The Vice President of Human Resources must approve all requests for retrieval or

reporting of IT collected data for a specific employee.

2.1.2. All requests for reporting of IT collected data for a specific employee must be made

through the Chief Information Officer (CIO).

2.1.3. All requests for IT collected data must be for individual employees, and not for a

department or portions of a department.

2.1.4. All requests for IT collected data from any and all affiliates (LCA, TRBC, Sodexo, etc.)

must be made through the Chief Information Officer (CIO).

2.1.5. Any requests for data that may be disclosed publicly as the result of a criminal

investigation must be requested via a subpoena.

3.2. E-mail data.

3.2.1. Requests for viewing the contents of private e-mail sent or received by staff must be

approved by:

3.2.1.1. The Vice President of Human Resources

3.2.1.2. The Chief Information Officer

3.2.2. Requests for viewing the contents of private e-mail sent or received by faculty must be

approved by:

3.2.2.1. The Vice President of Human Resources

3.2.2.2. The Chief Information Officer

3.2.2.3. The Provost

#### 4. Use of retrieved data

4.1. If the retrieved data is being used for disciplinary action:

4.1.1. Before this data is to be used in support of disciplinary action, the data should be assessed

and reviewed for false positives due to software running in the background which does not

necessarily represent negative or unacceptable personnel activities. Examples of such

software include online music players, auto-refreshing applications and/or portals which

request information from the internet without action by the user, or other non-indicting

behaviors which do not violate our acceptable use policy or other related policies.

4.2. Data that is retrieved is to be delivered to Human Resources immediately upon retrieval.

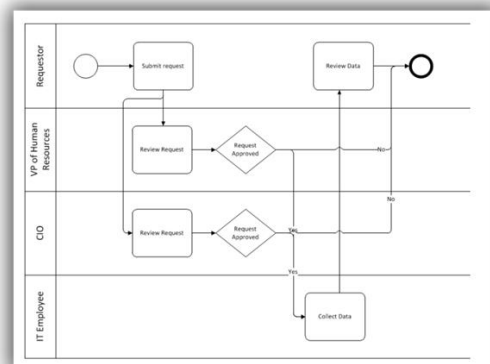
4.2.1. Human Resources will coordinate the dissemination of the retrieved data.

#### 5. Authority to retrieve data

5.1. The Director of IT Operations has the authority to determine which members of his staff have permission to retrieve the IT-collected data.

5.2. Employees with permission to retrieve IT-collected data are to view and/or retrieve this data

only when a formal, standardized request procedure has been submitted.



## Sanctions

1. Non-compliance to these documented standards may be communicated via e-mail to:

1.1. The IT employee's director

1.2. The Chief Information Office

1.3. The Vice President of Human Resources

## **Exceptions**

None