Procedure Cyber Security Training	**Last Update:** January 2020

References: County Policy Manual- Use of Information Technology Resources Policy Information Security Policy, all ISAC Standards

Purpose: To establish procedures, processes and outcomes on the proper use of Jefferson County Information Technology Resources.

A. Applicability

1. This Procedure shall apply to all Departments/Divisions that report to the Board of County Commissioners, Elected Officials and Appointed Officials and their Offices.

2. Covered Employees and Other Individuals.

3. Some County Departments/Offices may impose additional procedures, standards and other documents.

4. Employees may be required to confirm that they have read, understand and agree to abide by this Procedure, and any applicable policies, procedures, standards, and/or other documents.

B. Training

1. Minimally, each two months anyone with access to county technology resources will be notified of new cyber security awareness training.

2. Training will be delivered and completed within a training cycle, a two-month window

    a. The training cycle starts when the cyber security awareness training is delivered

    b. The training cycle finishes 60 days after training is delivered

    c. There will be 6 training cycles per year.

C. Testing

1. Minimally, four times per year the County will assess anyone with access to electronic mail by sending test phishing emails.

2. Alternative testing, such as phone phishing, USB and other portable media tests, may be delivered randomly throughout the year to anyone with access to information technology resources.

3. If anyone fails a test, the tool will notify the individual they have received and failed a County test.

4. Each time the employee or staff fails a test, additional training will be delivered to that individual. The additional training will be required to be completed within five business days from the time the failed test occurred. Follow up training will not exceed 30 minutes in duration. Follow up tests will be delivered each subsequent month until the test is passed.

C. Failure to Comply

1. On the Department, Division or Office level, failure to comply consists of the following:

   a. Does not maintain an 85% or better training completion rate during the training cycle, or

   b. Does not comply with 100% testing requirements, or

   c. Does not comply with County information security policies, procedures, standards and/or other documents

2. On the information technology resource user level, failure to comply consists of the following:

   a. An individual not completing training within the training cycle, or

   b. An individual failing 3 consecutive phishing tests, or

   c. An individual failing more than 5 phishing tests in 12 consecutive months, or

   d. An individual causing a loss of data or the spread of malicious software, or

   e. An individual putting the county at risk by failing to implement skills in taught in training i.e. falling for a phishing or other cyber attack

3. Failure of a department, division, or individual to comply will result in loss of privileges such as access to information technology resources and/or disciplinary action:

   a. Failure to comply with policy, procedure or standards will result in the loss of information technology privileges.

b. Failure to comply with policy, procedure or standards may result in disciplinary or corrective action taken by the division or department directors. Employees who do not demonstrate competency in protecting the County's information technology resources, such as not completing the training within the required timeframe, failing consecutive phishing tests, clicking on an actual phishing link or opening an attachment in a phishing email, may result in loss of information technology privileges, disciplinary or corrective action.

4. Restoration of technology privileges will require approval by the Chief Information Security Officer.