

Kids Central, Inc. System of Care Policy & Procedure

Series: General Services and Information Technology

Policy Name: Security Awareness Training

Policy Number: 1000

Origination Date: 08/29/06

Revision Date: 9/29/2010

Authority: Section 282.318, F.S., "Security of Data and Information Technology Resources", Chapter 815, F.S.; "Florida Computer Crimes Act"

Reference: COA Standard RPM 6.01; Standard Contract PJH04, paragraph W

Policy

It is the policy of Kids Central, Inc. to ensure the protection of confidentiality, integrity, availability, and reliability of all information technology resources used to support the needs of our clients and the missions of the organization. Each person who uses equipment to access data by means of information technology resources owned, purchased, or leased by Kids Central, Inc. will have a unique personal identifier (password). Prior to obtaining a password, the person must sign form CF 114 and complete the computer based Security Awareness Training course (within 10-days of employment for new hires)

Procedure

A. General Information on Security Awareness Training

1. The Kids Central Training Department will inform all new employees of the need to complete Security Awareness Training within 10 days of the employee having opportunity to access confidential information. Security Awareness Training is an annual requirement for all employees.
2. The Kids Central Training Department will track all Security Awareness Training to ensure that all new employees are trained and that the annual requirement is met.
3. The Security Awareness Training is available on-line at:
<http://www.dcf.state.fl.us/admin/training.shtml> and is designed to ensure that each employee is made aware of the relevant laws and policies pertaining to keeping data secure and confidential as well as the penalties proscribed for any violations of these laws and policies.
 - a. The employee will complete the training and print out a certificate of completion.
 - b. This certificate will be the only acceptable proof of training.

Kids Central, Inc. System of Care Policy & Procedure

- c. Other proof of training completion must be approved in advance by the Kids Central Security Officer.
4. If a Kids Central employee, volunteer or CMA employee has not completed the Security Awareness Training within 10 days the following procedure will be followed:
 - a. The Kids Central Data Security Officer will terminate the individual's access to all Kids Central data systems.
 - b. The Kids Central Data Security Officer will notify the DCF Security Officer of the need to terminate the individual's access to any DCF systems.
 - c. The Kids Central Data Security Office will notify the Chief Financial Officer of the need to terminate the individual's access to confidential information in any form.
 - d. The Chief Financial Officer will notify the Kids Central Director of Operations and the CMA Program Director of the need to terminate the individual's access to confidential information in any form.
5. Any employee failing to complete the training and who has been removed from access to all confidential information will have three days to complete the required training and provide proof of completion.
6. If the individual fails to complete the required training in the specified timeframe, the employee will be referred to the Chief Financial Officer with a recommendation to terminate their employment.
7. Upon notification of successful completion of Security Awareness Training the following will occur:
 - a. The Kids Central Data Security Officer will reinstate the individual's access to the Kids Central data systems.
 - b. The Kids Central Data Security Officer will notify the DCF Security Officer of the need to re-instate the individual's access to any DCF systems.
 - c. The Kids Central Data Security Officer will notify the Chief Financial Officer of the need to reinstate the individual's access to confidential information.
 - d. The Chief Financial Officer will notify the Kids Central Director of Operations or CMA Program Director of the need to reinstate the individual's access to confidential information in any form.

Approved By:


Cynthia A. Schuler, Chief Executive Officer

Date