Data Processing Procedures

Charlotte County Public Schools
Information and Communications System

The policies that govern Data Processing (DP) personnel in the Information and Communication System Department may be different from procedures used in other departments because of the nature of DP operations, therefore they a outlined in the following:

1.1 Recruiting and Selection Procedures

Every effort is made to discourage turnover in personnel in the Information and Communication Department (ICS). Time is provided in the hiring process to insure the best possible qualified employee is obtained. Recruiting and selection procedures are limited to "long term" employment. The Director of ICS works with HR personnel to ensure this process works to the highest level.

To obtain experienced personnel the following procedures for recruiting DP candidates are encouraged:

A. Members of the ICS Department will serve on the interview team to help recommend qualified persons who would fit into the organization. Members of the team are given additional time within their workday to evaluate and research candidates. If "after hours" time is needed, time will be given as "comp" time to repay their efforts. Upon the interviewing team recommendation of candidates, the Director of ICS will evaluate the selected recommendation, make recommendation to the HR Department and inform the team of the candidate he has recommended to HR.

B. The person leaving the position knows what is needed for the job therefore they will serve on the recruiting/interviewing team when possible.

C. HR personnel perform all background checks for candidates with assistance from the Director of ICS on pertinent issues. An extra degree of care shall be performed when Access Control personnel are being hired.

In ICS employee recruitment, there are environmental factors to be considered. One is the nature of "School Business", which is considerably different than the other business world. The nature of the working environment of programmers, data entry operators, and system analysis are all different for the "Education" environment. A prospective employee is recruited to fit the working climate within the ICS Department of Charlotte County Public Schools.

To ensure that job selection procedures are successful, the personal job characteristics required for effective job performance is specified by the position job description as held in the HR Departments Job description book for the District. These ICS descriptions are reviewed each year by the Director of ICS to ensure "currentness" to the actual position.

Test of candidate skills may also be provided by the ICS Department during the interview process. The Director of ICS develops the skill tests with assistance from the staff involved in the interview process.

1.2 Discipline and Termination Procedures

The procedures for discipline and termination are followed as outlined in School Board Policies with every effort being made not to jeopardize any future relations the employee may have with the Charlotte County Public Schools and the ICS Department. The efforts are also to ensure that no undo attention is brought to the employee or the department because of the nature of the business conducted. Employees, as will as department managers, are discouraged from discussing any discipline or termination issues with anyone not associated with Department and School Board inquiry.

The Director of ICS always conducts exit interviews with assistance from key ICS personnel when appropriate.

1.3 Performance Review

Performance reviews are conducted as described in School Board Policies on a regular bases in the ICS Department. Each area within the ICS framework has additional review processes to consider. They are:

A. Computer Operations: review of data entry volume per error ratio, based upon the nature of the data and documentation. Review of computer operations efficiency in running the computer systems processes assigned.

B. Programmers: review of productivity of creating processes within programs or new program structure. Performance reviews of programming staff are also assisted with the following: Peer Review, Time by Program Function, and client satisfaction with product created.

C. Records Retention Specialist: review of document archiving efficiency. Review of on task behaviors.

D. Secretary: review of confidentially commitment to process within the ICS department. Review of effectiveness in other assigned department task.

E. Program or System Analysis: review of effectiveness and efficiency of conducting assigned duties and review of Server reliability to the district and department.

Duties of Information and Communication System Employees:

All duties and responsibilities are outlined within the job descriptions for each position in the HR handbook of Job Descriptions. However, additional job responsibilities may be given to employees as directed by ICS management or the Superintendent of Schools. No ICS employee may take on additional responsibilities without the agreement of ICS management. No

unauthorized application/process(s) may be conducted without the written authorization of the Director of ICS or the Superintendent of Schools. School Board Policies apply to authorization of procedures in all cases.

Physical Security of Data Center and Communication Closets

1.1 Physical Security of Data Center:

There shall be limited access to ICS Data Center at all times. This shall include the closing and locking of outside doors at all times. No outside doors to ICS shell be left open or unattended. Only authorize personnel (those employees associated with ICS or Learning Though Technology) shall be permitted to enter the ICS Data Center without authorize personnel acknowledgement/accompaniment. No unauthorized personnel shall be left unattended at any time while in the Data Center. No logs of unauthorized persons in Data Center during normal work hours need be kept.

During non-production hours, all of the ICS Data Center shall be secured by using Sonitrol Electronic Control System and their digital control access. This access is monitor by the Sonitrol Control Company during off hours and reports sent to ICS on all authorize entries for period on time of one month. These reports are reviewed by the Director of ICS on a regular base. Each employee has been provided a PIN number, which gives access to the Data Center during off hours. No employee is permitted to give others their access PIN number. If continued access is needed by an employee, arrangements for this work time are to be made with the Director of ICS – there shall be no unauthorized extended work time without the authorization of the Director of ICS.

All Facilities/closets storing network equipment shall be posted with restricted entry placards on the doors and the doors closed and secure at all times when not being access by ICS, LTT or District Maintenance personnel. The network/server closets shall be additionally secured by the ICS/LTT staff during times of threatening storms, such as hurricanes, with plastic covering above equipment.

Inventory is kept on all ICS equipment on the District Inventory System and all equipment is insured though the District affiliation with SCREMP.

1.1 Software Securities:

The ICS System Analysis is responsible to monitor UNIX, and FOCUS access activity during and after work hours. Reports are to be provided to the Director of ICS on a monthly base.

No employee in the ICS Department is permitted to install software on Charlotte County Public School equipment without the permission of ICS or LTT management. No employee in the ICS Department is permitted to connect his/her own computer equipment to district networks without permission of ICS or LTT management.

1.2 Disaster Recovery/Contingency Planning:

The ICS Department shall have a disaster recovery plan and a contingency plan in place. The Disaster Recovery Plan shall be evaluated by the ICS Steering Committee on yearly bases and upon recommendation from the committee the Plan shall be tested for proper functionality. ICS Personnel are to be trained on Disaster Recovery procedures and their individual responsibilities during the test phase of the Disaster Recovery Plan.

The Disaster Recovery Plan shall include:

A. An off-site storage location
B. An off-site Access Control procedure for data security
C. A written emergency plan addresses of all vital locations
D. Suitable backup procedures which can reproduce all data functions
E. Critical applications are Bi-tech and FOCUS. All other not consider critical in the operation of District functions.
F. Priority of application processing will be Payroll, HR functions, Inventory, Purchasing and Student Data – with that order. All other function will take secondary priority.
G. The vendors assisting ICS with Disaster Recovery is:

Softwarenology
2590 Northbrook Plaza Dr.
Suite 106 Naples, Florida 34119
Phone: 239-260-7828
http://softwarenology.com

FOCUS School Software
475 Central Avenue
Saint Petersburg, Florida
Phone: 877-250-1771
http://focus-sis.org/index.php

An ICS Contingency Plan shall include the following:

A. Data files and program files are backed up each night by the night Computer Operator or established automated procedures.
B. Server system nightly backups
C. Remote storage of backup tapes at the Special Projects building in Punta Gorda on a weekly bases.

1.1 Computer Equipment:

All computer equipment used with the ICS department will be of the specification established by the District Technology Committee and reevaluated on annual bases.

1.1 System Development and Maintenance Control:

There shall be a formal system for requests for development and maintenance of systems and program software in the ICS department. This system will be called RDS (**R**equest for **D**evelopment **S**ystem). The RDS system is an electronic request process for development of software or revision of existing software. The RDS will be originated by the requestor or by ICS management. RDS requests shall involve project managers, system analysis, programmers, acceptance testers and users. Users are asked to activity participate in system development, updates and maintenance projects in the ICS department. All RDS requests shall include the following: date of request, request assigned number, reason for request, nature of effected changes, person requesting change, person doing the changes/modifications/updates, documentation of process, anticipated completion date, completion date and run documentation. In the beginning, all RDS request shall come to the attention of the Director of ICS for approval to proceed.

Upon completion of all program changes, and updates, each interrelated subsystems are thoroughly tested. Comparison procedures between data before the changes and data possibility affected after the change shall be used. When possible, all changes or updates shall be tested in a test environment in parallel with the "old software". "Acceptance testing" shall be performed to ensure that performance is in accordance with functional and detailed specifications, including desired controls, and that it meets the user's needs and objectives. When possible, all RDS request products shall be evaluated by other District departments for desired performance. After testing, data comparison and upon completion of RDS process, the RDS shall come back to the attention of the Director of ICS for final approval before put into production by the System Analysis of ICS. All authorizations for placing into production are do be done in writing and filed in the ICS control center.

Run documentation for RDS product shall include a brief description of the system/program/change /update, description and examples of all input and output, listing of program code, instruction for control parameters, lists of messages, halts, and necessary actions for operation, estimated normal and maximum run times, recovery and restart procedures and explanation of expected output. The ICS System Analysis shall move into production upon authorization of the Director of ICS.

The RDS electronic system has replaced the previous paper RDS system. This system was developed within ICS and follows the same procedures for development as outlined above. The electronic system will use the same format for request for work, development, testing and acceptance and will as production implementation as described for the RDS electronic system.

Emergency program changes are/maybe exceptions to the above procedures with each situation being evaluated by the Director of ICS and his management staff. Upon review of the emergency, the Director of ICS for each circumstance will establish the necessary steps for action. The steps will be implemented and a reevaluation of the reason for the emergency will be performed.

1.1 <u>Access Control</u>:

Access to System and Program software as well as physical access to ICS function shall be implemented according to the following:

Access to program and operating system documentation shall be limited to employees or vendor employees who require the documentation for performance of the assigned responsibilities.

The Director of ICS and the ICS System Analysis shall be the Access Control Administrators and shall have the sole responsibility for access control. Background checks for Access Control Administrators shall be conducted in accordance to regular School Board Policy for performing regular background checks prior to hiring. On occasion, responsibility for access control may be passed on to Program Analysis while directly supervised by the Director of ICS or the System Analysis for reasons of emergency. All such occasions shall be of short duration – 30 days or less.

The duties of the Access Control persons shall be to limit access to necessary components of systems and programs to the user. These limits shall include programming, operations and clerical staff as well as end users in other departments. The System Analysis shall establish access and level of security for each user. The Director of ICS shall monitor access and levels of security and shall maintain a log of all users' levels and passwords. This log shall be kept and maintained in a secure manner. No School District employee is allowed to use the computer equipment used by the System Analysis or the Director of ICS without the expressed approval of the System Analysis or the Director of ICS. Approval for use of said equipment may only be given on a case-by-case as it happens.

For a user to establish access, a request for access must be made by the user's direct supervisor. No level of access will be granted without a written request from the supervisor of the proposed user. No changes in access will be granted without the written request of the user's supervisor. The ICS System Analysis shall create all passwords for users. The user shall have the right to change their password; however it shall remain the responsibility of the user to maintain the security of his/her password at all times in accordance with School Board Policy. All passwords, which permit access to secure area, shall be changed upon termination of employee affecting that area. The ICS System Analysis, upon termination of an employee, shall remove access accounts given to those employees during employment.

When possible the internal security software provided within the UNIX system, the Bi-tech and FOCUS application and that provided by the Novell network/server software will be employed by the ICS System Analysis and Director to appraise the access abilities of users and to evaluate the vulnerability of the ICS software. Audit trials within program procedures and system logs will be periodically reviewed by the ICS System Analysis and Director for unauthorized use or deployment of software within the ICS functional domain. If unauthorized entry is discovered, it is the responsibility of the Director of ICS to notify the Assistant Superintendent of Human Resources and Employee Relations and to notify other Directors, which may have, compromised data.

All connect methods to the ICS network and servers shall be monitor for possible unauthorized intrusion. All external connections to the ICS network are protected by the District's Firewall. All system and program backup methods shall be maintained in a manor that will discourage and prevent unauthorized access. All computers within the ICS domain shall be protected with anti-virus software. This software shall be kept up-to-date and "active" at all times. The Director of ICS may grant exceptions to anti-virus active engagement on case-by-case bases.

2.1 Data Classification and Handling Policy

Purpose

The purpose of this policy is to establish a framework for classifying and handling Charlotte County Public Schools data based on its level of sensitivity, value and criticality to the Charlotte County Public Schools as required by the Charlotte County Public Schools' Information Security Plan as stated herein. Classification of data will aid in determining baseline security controls for the protection of data.

Scope

This policy applies to all Charlotte County Public Schools employees who access, process, or store sensitive District data.

Definitions

Confidential Data- Generalized term that typically represents data classified as confidential, according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.

Data Owner- An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of the Charlotte County Public Schools. See the Information Security Roles and Responsibilities within this document for more information.

Data Custodian- Any employee of the Charlotte County Public Schools who has administrative and/or operational responsibility over informational assets. See the Information Security Roles and Responsibilities document table for more information.

Institutional Data- All data owned or licensed by the Charlotte County Public Schools

Information Assets- Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to the Charlotte County Public Schools

Non-public Information- Any information that is classified as Internal/Private Information according to the data classification scheme defined in this document.

Sensitive Data - Generalized term that typically represents data classified as Confidential according to the data classification scheme defined within this document.

2.2 Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the Charlotte County Public Schools should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels (tiers), or classifications:

Tier1-Confidential Data

Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the Charlotte County Public Schools or its affiliates. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied.

Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the Charlotte County Public Schools who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be individually requested and then authorized by the Data Owner who is responsible for the data.

Tier 1 Confidential data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Confidential/Restricted data include official student grades and financial aid data, social security and credit card numbers, and individuals' health information.

Tier 2-Internal/Private Data

Data should be classified as Internal/Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the Charlotte County Public Schools or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data.

Access to Internal/Private data must be requested from, and authorized by, the Data Owner who is responsible for the data. Access to Internal/Private data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by department/school administration.

Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the Charlotte County Public Schools should this information not be available when needed is typically moderate. Examples of Internal/Private data include official Charlotte County Public Schools records such as financial reports, human resources information, some research data, unofficial student records, and budget information.

Tier 3-Public Data

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the Charlotte County Public Schools and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected. The appropriate Data Owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Level 3 Public data not be available is typically low, (inconvenient but not debilitating). Examples of Public data include directory information, course information and research publications.

2.3 Data Collections

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address and social security number, the data collection should be classified as Confidential because of the social security number, even though the student's name and address may be considered Public information.

2.4 Determining Classification

The goal of ICS, as stated in the Charlotte County Public School's Information Security Plan herein, is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the Charlotte County Public Schools if confidentiality, integrity or availability of the data is compromised.

	POTENTIAL IMPACT		
Security Objective	Tier 3 Low	Tier 2 Moderate	Tier 1 High
Confidentiality- *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity- *Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.*	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability- *Ensuring timely and reliable access to and use of information.*	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

2.5 Predefined Types of Confidential/Restricted Information Assets

Based upon state, federal, and contractual requirements that is bound by, the following information assets have been predefined as Level 1 or Level 2 data and must be protected:

Personally Identifiable Education Records-Covered under FERPA

Personally Identifiable Education Records are defined as any education records that contain one or more of the following personal identifiers:

- Student CCPS ID Number
- Grades, GPA, Credits Enrolled
- Social Security Number
- Race/Gender
- A list of personal characteristics or any other information that would make the student's identity easily traceable

Personally Financial Identifiable Information (PIFI) - Covered under GLBA

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- Date of Birth
- Financial account number in combination with a security code, access code or password that would permit access to the account

Payment Card Information- Covered under PCI

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

Protected Health Information (PHI) - Covered under HIPAA

PHI is defined as any "individually identifiable" information that is stored by a Covered Entity, and related to one or more of the following:

- Past, present or future physical or mental health condition of an individual.
- Provision of health care to an individual.
- Past, present or future payment for the provision of health care to an individual.

PHI is considered "individually identifiable" if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Telephone/Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic that could identify an individual

If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe that the information can be used to identify an individual, it is not considered "individually identifiable" and; as a result, would not be considered PHI.

2.6 Data Security: Handling Requirements

For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability.

The following table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	**Data Classification**		
	Tier 3-Public	Tier 2-Internal	Tier 1-Confidential
Access Controls	No restriction for viewing Authorization by Data Owner or designee required for modification; supervisor approval also required if not a self-service function	Viewing and modification restricted to authorized individuals as needed for business-related roles Data Owner or designee grants permission for access, plus approval from supervisor	Viewing and modification restricted to authorized individuals as needed for business-related roles Data Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access
Copying/Printing (applies to both paper and electronic forms)	No restrictions	Data should only be printed when there is a legitimate need Copies must be limited to individuals with a need to know Data should not be left unattended on a printer/fax May be sent via Campus Mail	Data should only be printed when there is a legitimate need Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement Data should not be left unattended on a printer/fax Copies must be labeled "Confidential" Must be sent via Confidential envelope; data must be marked "Confidential"

Network Security	May reside on a public network Protection with a firewall recommended IDS/IPS protection recommended Protection only with router ACLs acceptable	Protection with a network firewall Required IDS/IPS protection required Protection with router ACLs optional Servers hosting the data should not be visible to entire Internet may be in a shared network server subnet with a common firewall rule set for the set of servers	Protection with a network firewall using "default deny" rule set required IDS/IPS protection required Protection with router ACLs optional Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the schools and guest wireless networks Must have a firewall rule set dedicated to the system The firewall rule set will be reviewed periodically
System Security	Must follow general best practices for system management and security Host-based software firewall recommended	Must follow Charlotte County Public Schools-specific and OS-specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended	Must follow Charlotte County Public Schools-specific and OS-specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended
Virtual Environments	May be hosted in a virtual server environment all other security controls apply to both the host and the guest virtual machines	May be hosted in a virtual server Environment all other security controls apply to both the host and the guest virtual machines Should not share the same virtual host environment with guest virtual servers of other security classifications	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Cannot share the same virtual host environment with guest virtual servers of other security classifications

Physical Security	System must be locked or logged out when unattended Host-based software firewall recommended	System must be locked or logged out when unattended Hosted in a secure location required; a Secure Data Center is recommended	System must be locked or logged out when unattended Hosted in Secure Data Center required Physical access must be monitored, logged, and limited to authorized individuals 24x7
Remote Access to systems hosting the data	No restrictions	Access restricted to local network or VPN remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet	Restricted to local network or secure VPN group unsupervised remote access by third party for technical support not allowed Two-factor authentication recommended
Data Storage	Storage on a secure server recommended Storage in a secure Data Center recommended	Storage on a secure server recommended Storage in a secure Data Center recommended Should not store on an individual's workstation or a mobile device	Storage on a secure server required Storage in Secure Data Center required Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption Encryption on backup media required Paper/hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	No restrictions	No requirements	Encryption required (for example, via SSL or secure file transfer protocols) Cannot transmit via e-mail unless encrypted and
Backup/Disaster Recovery	Backups required; daily backups recommended	Daily backups required Off-site storage recommended	Daily backups required Off-site storage in a secure location required

Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	No restrictions	Recycle Reports; Wipe/erase media	Shred reports Destruction of electronic media
Training	General security awareness training recommended	General security awareness training Required Data security training required	General security awareness training Required Data security training required Applicable policy and regulation training required
Auditing	Not needed	Logins	Logins, access and changes
Mobile Devices	Password protection recommended; locked when not	Password protected, locked when not in use	Password protected, locked when not in use, encryption used for Level 3 data

3.1 Data Incident Response Plan

The following discusses the steps taken during any data critical incident response.

The person who discovers the incident will call the ICS office. Persons discovering the data critical incident may include, but not limited, to the following:

a) Intrusion detection monitoring personnel
b) The system administrator
c) The firewall administrator
d) A software business partner
e) ICS data department personal,
f) School data managers, and student registers,
g) District administrators and administrative support personal,
h) Teachers, and councilors
i) The security department or a security person.
j) An outside source

The above personal has access to the data in the district and may effectively discover a potential data incident any time day or night.

When an incident is suspected the individuals is required to contact the Director of ICS or the District's System Analysis to report the suspected incident. If reporting cannot be made to these people, contact must be made to one of the three the District's Assistant Superintendents and/or their administrative assistant for them to report to the ICS Director or System Analysis as soon as possible.

Any person reporting a suspected critical incident may contact 941-255-0808 ext. 9091 or 941-815-7119 which is reachable 24/7. Any member of the ICS staff may use the emergency phone tree provided each school year.

1) If the person discovering the incident is a member of the ICS department or affected department, they will proceed to step 4.
2) If the person discovering the incident is not a member of the ICS department or LTT department, they will call the one of the 24/7 reachable numbers provided above.
3) The District security office will refer to the ICS emergency contact list or effected department contact list and call the designated numbers in order on the list. The person receiving notification will log:
    a) The name of the caller.
    b) Time of the call.
    c) Contact information about the caller.
    d) The nature of the incident.
    e) What equipment or persons were involved?
    f) Location of equipment or persons involved.
    g) How the incident was detected.
    h) When the event was first noticed that supported the idea that the incident occurred.
    i) This information will be transferred to the ICS director as soon as possible.
4) The ICS staff member or affected department staff member who receives the call (or discovered the incident) will refer to their emergency contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted as applicable. The staff member will log the information received in the same format as the ICS office in the previous step. The staff member could possibly add the following:
    a) Is the equipment affected business critical?
    b) What is the severity of the potential impact?
    c) Name of system being targeted, along with operating system, IP address, and location.
    d) IP address and any information about the origin of the attack.

5) Contacted members of the ICS/LTT response team will meet or discuss the situation over the telephone and determine a response strategy.
    a) Is the incident real or perceived?
    b) Is the incident still in progress?
    c) What data or property is threatened and how critical is it?
    d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    e) What system or systems are targeted, where are they located physically and on the network?
    f) Is the incident inside the trusted network?
    g) Is the response urgent?
    h) Can the incident be quickly contained?
    i) Will the response alert the attacker and do we care?
    j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.
6) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
    a) Category one - A threat to public safety or life.
    b) Category two - A threat to sensitive data
    c) Category three - A threat to computer systems
    d) Category four - A disruption of services
7) Team members will establish and follow one of the following procedures basing their response on the incident assessment:
    a) Worm response procedure
    b) Virus response procedure
    c) System failure procedure
    d) Active intrusion response procedure - Is critical data at risk?
    e) Inactive Intrusion response procedure
    f) System abuse procedure
    g) Property theft response procedure
    h) Website denial of service response procedure
    i) Database or file denial of service response procedure
    j) Spyware response procedure.

The team may create additional procedures which are not foreseen in this document as necessary. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

8) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

9) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

10) Upon management approval, the changes will be implemented.

11) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

    a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.

    b) Make users change passwords if passwords may have been sniffed.

    c) Be sure the system has been hardened by turning off or uninstalling unused services.

    d) Be sure the system is fully patched.

    e) Be sure real time virus protection and intrusion detection is running.

    f) Be sure the system is logging the correct events and to the proper level.

12) Documentation—the following shall be documented:

    a) How the incident was discovered.

    b) The category of the incident.

    c) How the incident occurred, whether through email, firewall, etc.

    d) Where the attack came from, such as IP addresses and other related information about the attacker.

    e) What the response plan was.

    f) What was done in response?

    g) Whether the response was effective.

13) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

14) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

15) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

16) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

    a) Consider whether an additional policy could have prevented the intrusion.

    b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

    c) Was the incident response appropriate? How could it be improved?

    d) Was every appropriate party informed in a timely manner?

    e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

    f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

    g) Have changes been made to prevent a new and similar infection?

    h) Should any security policies be updated?

    i) What lessons have been learned from this experience?