

**FRANKLIN COUNTY FINANCE DEPARTMENT  
DISASTER RECOVERY OVERVIEW**

**LEGAL RESPONSIBILITY:** Protection of personnel, assets, and resources is paramount.

**FINANCIAL LOSS:** The Finance Department is dependent upon the efficiency, accuracy and timely output of electronic data processing functions for its daily operations. If EDP is disrupted, Franklin County could be exposed to a loss of the records of financial assets, incurred liabilities, and revenues.

**INTERRUPTION OF SERVICES:** Franklin County employees, vendors and individuals that require our services could be adversely affected.

There are three levels of disaster recovery that are addressed in this plan: mandatory procedures, necessary procedures, and desirable procedures.

**MANDATORY PROCEDURES:** Those Procedures that relate to fire control, alarm systems, evacuation procedures, and the overall protection of the people that may be in the area as well as the assets of the office.

**NECESSARY PROCEDURES:** Those precautions that have been taken to prevent serious disruptions in the flow of the operations of the Finance Department

**DESIRABLE PROCEDURES:** Reasonable precautions that have been taken to prevent extended disruption in the operations of this office.

With these procedures implemented, we hope to minimize interruptions in daily operations, limit extended disruption and/or damage, and minimize economic impact. Alternative means of operation will be made apparent to personnel so they will be prepared for emergency situations and be able to restore operations in a timely manner.

## **FRANKLIN COUNTY FINANCE DEPARTMENT OFFICE DESCRIPTION**

The Franklin County Finance Department was established to provide for a centralized accounting system for all functions of Franklin County Government, including the General Fund, Solid Waste/Sanitation Fund, Highway Fund, Schools General Projects Fund and Schools Federal Projects Fund, as well as other miscellaneous funds for the County.

Employee payrolls are generated for all County and BOE employees. Retirement is generated for all offices, and retirement records are maintained for all employees. Employee insurance records and personnel files are kept for all employees. Financial accounting records are generated in this office, and all financial records for Franklin County are stored in this building, as well as some Circuit/General Sessions Court records that are stored in the building in a separate room. All checks, both payroll and vendor, are generated by the Finance Department and check stock for all funds are stored in this building in a secured area. Purchase orders are generated by the Finance Department, and all records relating to the required bid process are stored in a locked file cabinet. All accounts payable records, including copies of the requisition, purchase order, invoice and check are filed alphabetically by vendor name.

### **BUILDING DESCRIPTION**

The Franklin County Finance Department is housed in a separate building that previously housed the Franklin County High School Vocational Rooms. It has been completely renovated, and is a single story building. All floors are cast-in-place concrete slabs. Interior load bearing walls are 8” concrete masonry units. Exterior walls are load bearing concrete masonry units with brick veneer facing. The majority of the roof structure is conventional steel bar joists and metal deck supported on load bearing masonry walls. A portion of the roof structure, over the back portion of the offices is poured-in-place concrete supported on concrete beams and columns. The roofing material was redone during the renovation process, as well as completely new wiring, electrical outlets, light fixtures and HVAC units as needed. The finance office is protected by an alarm system which is controlled by management and connected to a security monitoring service; all locks for the building are installed by an outside vendor, and keys are controlled by management. The offices are equipped with smoke alarms in the building, as well as five motion detectors which are linked to the security system. Doors to all offices are closed and locked at the end of each work day.

**SOFTWARE SYSTEMS UTILIZED:**

**LOCAL GOVERNMENT DATA PROCESSING CORP.**

NextGen Accounting  
FlexGen Payroll  
FlexGen Purchasing  
FlexGen Accounts Payable  
FlexGen Fixed Assets  
Image Ease

**MICROSOFT OFFICE 2010**

Word  
Excel  
Access  
Outlook  
Publisher

**ADOBE ACROBAT**

**SIESTA SOFTWARE**  
(add-on for Payroll)

**VIRUS & MALWARE**  
AVG CloudCare  
Malware Anti-Malware Premium

**CHECK STOCK VENDORS**

TOPS Forms, Inc. (877)895-2284

**SOFTWARE VENDORS**

|                                  |                |
|----------------------------------|----------------|
| Local Government Data Processing | 1-800-737-1826 |
| Siesta Software                  | 1-423-653-4787 |

## **MANDATORY PROCEDURES**

The safety of the personnel and assets of the Franklin County Finance Department is, in large part, protected by the construction of the building itself.

There are smoke detectors in all areas of the building and employees have discussed an emergency evacuation procedure.

All employees have been instructed in the arming and disarming procedures for the security system as well as all areas to check before closing the building.

There is a fire resistant file cabinet in the building for additional protection of vital records.

All data is backed up on a daily basis (both the network server and the UNIX server) and the tapes are taken to an off-site location each morning.

## **NECESSARY AND DESIRABLE PROCEDURES**

1. Employees are provided with, and encouraged to use, memory stick storage devices for those files they generate with the Microsoft Office and other general products. These memory sticks are to be removed and kept with the employee when not in use.
2. One copy of the MS Office CD has been stored in a secure, off-site location, along with a listing of the registration numbers for each computer.
3. Paper copies of Audit and Budget documents for previous years are stored in a secure, off-site location.
4. Network access and system software passwords will be recorded (as well as required changes) and forwarded to the network coordinator for storage in a secure, off-site location. This information will also be used to delete these access passwords in the event of employee termination.
5. Random Backup Disc are sent to Local Government Data Processing Corporation for verification of backup success on a bi-annual basis.
6. A finance department inventory list is updated and kept with this policy at an off sight location for reference and safekeeping.
7. The finance director reviews monthly the Audit History Reports and keeps in a binder labeled "Franklin County Audit Changes"
8. The computers, hardware, software, & network are purchased and maintained through Local Government Corporation. Passwords are not kept on file for security purposes. If issues arise and an individual needs help accessing their data & network, LGC is contacted and completes the

process to get the employee back running, passwords are changed in FlexGen and Next Gen every ninety (90) days.

9. Individual computers are set to go to sleep after non-use in 30 minutes, to prevent non-valid user tampering. The correct user password is required to log back in.
10. The LGC Network Server, Image Ease Server, and Edge Email Server are kept in an atmosphere controlled environment under lock and key. Keys are kept hidden in the finance director's office.

### **PROCEDURES FOR IMPLEMENTING RESUMPTION OF BUSINESS**

1. Notify the Director of Emergency Management (see phone listing attached) of the nature and extent of the disaster and, if necessary, request use of the EMA facilities as an alternate operations site.
2. Notify the Local Government Data Processing (see phone listing attached) of the nature and extent of the disaster and request emergency assistance for the EDP portion of the recovery process.
3. Confirm the details of the notifications in writing within 48 hours.
4. Begin making necessary arrangements to acquire and/or move needed computer equipment, supplies, forms, etc. to the alternate site. If necessary, notify all employees of the alternate site location.
5. Confirm that all needed system backup media has been secured and taken to the alternate site for restoration.
6. Prepare requisitions and purchase orders as needed for equipment and software needed for restoration of office functions.
7. Supply personnel with the necessary procedures to begin restoring the system.
8. Review for completeness the materials transferred to the alternate processing site.
9. Begin restoring the system from backup media.
10. Begin normal operations as soon as possible.

## **DISASTER RECOVERY CHECKLIST**

The following list will assist in a disaster recovery process:

- 1) Notify management of the situation.
- 2) Set up and contact a disaster recovery team.
- 3) Determine the severity of the disaster.
- 4) If needed, contact the area for the temporary site and establish a schedule for utilization.
- 5) Contact all personnel
- 6) Contact all vendors (Hardware and Software)
- 7) Notify the insurance company. (Agent is currently V. R. Williams)
- 8) Notify all vendors that are currently associated with the County to expect a delay because of disruption of services.
- 9) Organize and determine tasks for each member of the recovery team.
- 10) Obtain emergency operating supplies.
- 11) Provide for the rental or purchase of computer equipment as needed.
- 12) Coordinate the delivery and receipt of mail and couriers.
- 13) Determine software application restoration priorities.
- 14) Retrieve current system backup. (Daily-Located at the Trustee's Office in the County Courthouse, Qtrly- Located at SunTrust Bank Lock Box)
- 15) Restore system.
- 16) If necessary, establish priorities for use and/or working hours for employees.

Use of the attached schedules will facilitate the notification process as well as the restoration process and insurance claim procedure. These are as follows:

- a) Building and Emergency Exit Plan
- b) Employee Phone Numbers and Addresses
- c) Emergency Phone Numbers
- d) Other Phone Numbers
- e) Current Finance Department Inventory

**EMPLOYEE PHONE NUMBERS AND STREET ADDRESSES**  
 (\* indicates member of disaster recovery team)

|  |   |
|--|---|
| * ANDREA SMITH<br>1715 Water Cure Rd<br>Winchester, TN 37398<br>(931)967-8618 Home     | Finance Director<br><br>(931)581-7948 Cell        |
| * CINDY LATHAM<br>538 Buncombe Rd.<br>Belvidere, TN 37306<br>(931)967-2049 Home        | Deputy Finance Director<br><br>(931)308-9133 Cell |
| ANNETTE SISK<br>595 Mansford Rd.<br>Winchester, TN 37398<br>(931)967-3399 Home         | HR Specialist<br><br>(931)580-9206 Cell           |
| JENNY PHILLIPS<br>15940 David Crockett Hwy<br>Huntland, TN 37345<br>(931)469-0274 Home | Payroll<br><br>(931)808-1011 Cell                 |
| PATTY CUSTER<br>677 Pine Bluff Rd.<br>Winchester, TN 37398<br>(931)967-6912 Home       | Payroll<br><br>(931)636-0231 Cell                 |
| HEATHER MORGAN<br>1468 Williams Cove Rd<br>Winchester, TN 37398<br>(931) 349-4474 Cell | Payroll   |
| AMY SMITH<br>6675 Old Alto Rd<br>Decherd, TN 37324<br>(931)636-5803 Cell               | Accounts Payable                                  |
| BECKY COWAN<br>633 Riley Lane<br>Winchester, TN 37398<br>(931)308-7408 Cell            | Accounts Payable                                  |
| CINDY MARSHALL<br>111 Warren Chapel Dr<br>Decherd, TN 37324<br>(931)967-5243 Home      | Accounts Payable<br><br>(931) 691-4178 Cell       |
| LILA WILKINSON<br>127 Chase Circle<br>Winchester, TN 37398<br>(931)967-4527 Home       | Accounts Payable<br><br>(931)636-7016 Cell        |

## EMERGENCY PHONE NUMBERS

FRANKLIN COUNTY MAYOR: Richard Stewart  
OFFICE: (931)967-2905  
HOME: (931)967-2429  
CELL (931)308-1578

FRANKLIN COUNTY I/T COORDINATOR: Tim Armstrong  
OFFICE (931)962-2106  
CELL (931)691-9672

EMERGENCY MANAGEMENT DIRECTOR: R. Eric Trussell  
OFFICE (931)967-4532  
HOME (931)962-2844  
CELL (931)308-9005

EMERGENCY SERVICES 911

TENNESSEE EMERGENCY MANAGEMENT AGENCY 1-800-533-7343  
WEST TENNESSEE 1-800-322-7341

TENNESSEE HIGHWAY PATROL  
DISTRICT OFFICE/EMERGENCIES ONLY 821-5151  
OTHER CALLS 821-3581  
FAYETTEVILLE 433-2179  
SHELBYVILLE 684-3234

NATIONAL GUARD (931)967-4581

SOFTWARE VENDOR Local Government Data Processing 1-800-737-1826  
Siesta Software 1-423-653-4787

FORMS VENDORS TOPS Forms, Inc. (877)895-2284

LOCAL INS. AGENT V.R. Williams & Co. (931)967-2268



## **SYSTEM STARTUP & SHUTDOWN PROCEDURES**

### **Startup**

1. As a rule the servers utilized by the finance department are kept on at all times and only shut down due to maintenance. Turn the server or computer in question on.
2. Utilize correct user name and password for server that are kept on file with the finance director.
3. If software is not working properly contact Local Government Corporation (1-800-737-1826) for assistance. Servers are under maintenance contract and if they are incapacitated or not working properly they will deliver or connect to a computer that is working properly to install the necessary software and backup to resume service to the finance department.
4. Servers are shut down about 6 times per year, due to updates or maintenance from Local Government Corporation staff.

### **Shutdown**

5. To shut down the server for maintenance. Exit out of all open programs.
6. Click on the Startup Tab.
7. Click on the Shutdown Tab
8. Click on the option to shut down due to maintenance tab
9. Click yes to continue, Watch and make sure the server actually does shut down.

## **DAILY, MONTHLY & YEAR-END ROUTINES**

### **Daily**

1. The backup log is checked for verification of a proper run from the night before.
2. Tapes are removed
3. Tapes are taken to the Trustee office and kept in a secure cabinet.
4. Tapes are retrieved for the next evenings run of back up.
5. Tapes are inserted into the backup device.

### **Monthly**

There are no procedures other than closing books and checking “Audit Change History Reports”

### **Year-End**

1. At year end prior to closing books a daily backup is processed.
2. The backup disc is taken to the Trustee’s office and kept in a secure cabinet.
3. Virus and Malware Software are updated annually with new license numbers by Local Government Corporation on each device.