Fraud, Theft, Blackmail, Vandalism, and Looting

Computers are password protected.

Vital records are locked when not in use.

Equipment and asset serial numbers are documented, and the documentation is   
maintained in an off-site location.

Sabotage

Locations of critical operations centers are not publicized, and the facilities are   
inconspicuous.

Personnel policies require the immediate removal from the premise of any employee reasonably considered a threat and the immediate revocation of their computer and facility access privileges.

Locked doors, motion detectors, or other controls restrict physical access to   
premises to authorized personnel.

Fire

Evacuation plans are posted in prominent locations and designate an outside meeting place so that personnel can be accounted for in an emergency.

Personnel is trained to secure or remove vital records if time permits.

Fire extinguishers and hoses are readily accessible.

Fire alarm boxes and emergency power switches are clearly visible and   
unobstructed.

Dry pipe sprinkler systems are installed appropriately and are the type that are staged with time for operator intervention before power shut down and activation.

Personnel are trained for sprinkler system intervention in the event of a false   
alarm.

Waterproof covers are located near sensitive equipment if   
sprinklers are activated.

Heat or smoke detectors are installed in ceilings, exhaust ducts, and under raised flooring and are in working condition.

**This model form/template must be customized to meet your Agency’s needs.**

Equipment is grounded correctly to protect against electrical hazards.

Lightning rods are installed as appropriate.

Local fire inspectors are engaged in building preparation and training of   
personnel.

Floods

A determination has been verified as to whether or not the facility is or is not in a flood zone.

Critical records and equipment are not located on the ground floor if the facility has more than one floor. (Vital records are located \_\_\_\_\_\_\_\_\_\_\_\_\_\_).

If the facility has only one floor and is located in a flood zone, raised flooring has been installed and wiring and servers are elevated several inches off the ground.

If there is another floor above the computer or equipment room, the ceiling above is sealed to prevent water damage.

Severe Weather

Early warning systems are monitored periodically.

Air Contaminants

Evacuation plans include shutting down the HVAC systems.

Telecommunications Failure

An alternate form of communication is readily available if local phone systems become inoperable. (*Insert alternate information here*).

End-to-end trace of telephone circuits to identify single points of failure such as a   
common switch, router, PBX, or central telephone office.

Management is aware of whether it qualifies for government-sponsored expedited restoration of telecommunications services through Telecommunications Service Priority Systems (TSPS), Government Emergency Telecommunications Service (GETS), or Wireless Priority Service Program (WPS), and has pre-arranged for such services in the event of an emergency. (ATA is not eligible as it is not classified as a critical business in the event of an emergency, such as a hospital).

Power Failure

Voltage entering the computer room is regulated to prevent power fluctuations.   
(Isolation transformers filter out spikes but not surges. Surge suppressors are built into the UPS systems).

An uninterruptible power supply (UPS) is in use with the computer system and has sufficient capacity to provide ample time to shut down the system in an orderly fashion and ensure that no data is lost or corrupted. (Power capacity would provide for \_\_\_\_\_\_ of normal operations plus shut downtime).

Other alternate sources of power such as generators are available and in   
working order.

If a generator is available, then an ample supply of fuel is on hand for   
replenishment.

A priority list is maintained to determine which equipment and facilities should be   
powered up and whether certain operations should be scaled back.

Alternate power supplies receive periodic maintenance and testing to maintain   
operability.

Local ordinances relative to the location of generators and the storage and delivery of fuel are understood and followed.

Equipment and Software Failure

Temperature and humidity control systems are in place along with alarm or detecting devices.

Data, operating systems, software applications, utility programs, and databases are backed up regularly using a grandfather-father-son method and are rotated to an off-site location at least daily.

Policies for labeling, listing, transporting, and storage of back-ups are documented and followed.

Software applications are inventoried, and related documentation is kept off-site.

Two copies of the operating system are backed up with one copy kept in the software library and the other kept in an off-site location.

Two copies of the proprietary software one copy kept in the software library and the other copy, including the source code, is kept in an off-site location.

Two copies of utility systems are backed up with one copy kept in the software library and the other kept in an off-site location.

Off-site storage is fire-resistant, environmentally controlled, and restricts physical access to authorized personnel. (Off-site storage is located at\_\_\_ \_\_\_\_\_\_\_\_\_\_\_).

Pandemic Event

Potential outbreaks are monitored periodically and tracked according to first outbreak overseas, first U.S. outbreak, first state outbreak, first county outbreak, first city outbreak, and first company outbreak.

Employees have access to soap and warm water and other hygiene tools for ongoing hygiene purposes.

Employees have read the Center for Disease Control and Prevention brochures “Cover Your Cough” and “Clean Your Hands”.

Procedures are documented for telecommuting if employees need to be kept separated.

Employees are cross-trained, and succession plans are in place.

Company policies regarding absenteeism and absentee pay during a pandemic event are clearly written and understood by employees.

Employee Safety

Employees have written procedures for reporting their safety status to a centralized location during a crisis.

Adequate reserves of bottled water are on hand in the event of an emergency.

Employees are furnished with an adequate supply of batteries to operate wireless devices, laptop computers, and other equipment in the event of a crisis.

Management is prepared with a supply of cash or a separate checking account with designated signers in the event of a crisis that shuts down the electronic payment systems (ATMs, credit cards, and debit cards will all be affected in this type of crisis).

Management has documented a plan for alternate transportation of critical services if a widespread disaster diverts normal transportation for humanitarian and other emergency efforts.