Regulations and Guidance

36 CFR 1223	Managing Vital Records
Federal Continuity Directive (FCD) 1	Federal Executive Branch National Continuity Program and Requirements
Continuity Guidance Circular (CGC)	Continuity Guidance Circular

Other Sources of Information

- The National Archives and Records Administration: Resources-Vital Records and Records Disaster Mitigation and Recovery: www.archives.gov/records-mgmt/vital-records/.
- Your state archives are a good source of information and assistance. To locate your state archives, visit: www.statearchivists.org/connect/resources-state/.

About FEMA's National Continuity Programs

Serving as the Nation's center of excellence for continuity planning, guidance, and operations, FEMA National Continuity Programs (NCP) executes its vision to ensure essential functions of government continue at all levels. Our mission is to safeguard the implementation of Executive Branch continuity and assist the continuity planning efforts of federal, state, local, tribal, and territorial government and non-governmental stakeholders to sustain the continuous performance of essential functions and critical services under all conditions. To accomplish this, NCP provides guidance, technical assistance, planning, training, and workshop support to other Department of Homeland Security (DHS) and FEMA components, federal departments and agencies, state, local, territorial, and tribal (SLTT) governments, and other members of the whole community, to include private sector owners and operators of critical infrastructure.

Contact Information

For more information, please contact FEMA NCP. For FEMA Region-specific information, contact the appropriate Regional Continuity Manager from the list below.

FEMA Region	Location
FEMA HQ	National Capital Region
Region I	CT, MA, ME, NH, RI, VT
Region II	NJ, NY, PR, VI
Region III	DC, DE, MD, PA, VA, WV
Region IV	AL, FL, GA, KY, MS, NC, SC, TN
Region V	IL, IN, MI, MN, OH, WI
Region VI	AR, LA, NM, OK, TX
Region VII	IA, KS, MO, NE
Region VIII	CO, MT, ND, SD, UT, WY
Region IX	AZ, CA, HI, NV, Pacific Territories
Region X	AK, ID, OR, WA

Regional offices may be contacted via:
FEMA-CGC@fema.dhs.gov

Website

Continuity news, tools, guidance, and other useful resources can be found on our website at: www.fema.gov/national-continuity-programs.

Continuity Essential Records Management

National Continuity Programs

July 2018

FEMA

What is Essential Records Management?

The identification, protection, and ready availability of information systems and applications, electronic and hardcopy documents, references, and records needed to support essential functions during a continuity event.

Critical supporting activities include:

- Appointing an Essential Records Manager.
- Identifying and protecting records necessary for the organization to continue continuity operations including performance of essential functions and reconstitution of normal operations.
- Conducting a Risk Assessment and a Business Impact Analysis (BIA) to identify the most vulnerable records and how to protect them.
- Ensuring continuity personnel have appropriate access at alternate locations to required media (e.g., paper, photographic film, microform, and/or electronic forms), equipment, and instructions for retrieval of essential records including, but not limited to, records stored in cloud-based applications and accessed via the Internet or a Virtual Private Network.
- Developing procedures to routinely update essential records to ensure they always contain the most current information.

Major Categories of Essential Records

- Emergency Operating Records: Records essential to the continued functioning or reconstitution of an organization during and after an emergency.
- Legal and Financial Rights Records: Records essential to protect the legal and financial rights of the Government and individuals directly affected by its activities. Examples include: accounts receivable, social security, payroll, retirement, and insurance records. These records were formerly defined as ‘‘rights-and-interests’’ records.

What are Essential Records?

Information systems and applications, electronic and hardcopy documents, references, and records needed to support essential functions during a continuity event.

Essential Records include:

- Emergency/Continuity Plan;
- Standard Operating Procedures (SOP);
- Staff contact and assignment information, such as names, addresses, and phone numbers;
- Orders of succession and delegations of authority;
- Policies, procedures, directives, and systems manuals;
- List of credit card holders to purchase supplies;
- Maps and building plans;
- Personnel and payroll records;
- Customer records;
- Social Security and retirement records;
- Contracts and vendor agreements; and
- Licenses and long-term permits.

What is an Essential Records Packet?

An electronic or hard copy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency situation.

The packet should include:

- A hard or soft copy of Emergency Relocation Group (ERG) members with up-to-date telephone numbers;
- An inventory of essential records with their precise locations;
- Necessary access mechanisms;
- Alternate location information;
- Access requirements and lists of sources of equipment necessary to access the records (e.g., hardware and software, microform/microfilm readers, internet access, dedicated telephone lines);
- Lists of records recovery experts/vendors; and
- A copy of the organization’s continuity plans.

How Do I Protect my Essential Records?

Through a Risk Assessment and a BIA, organizations can determine the outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences for both primary and alternate facilities. Consider the vulnerability of those records deemed essential and take necessary steps to protect them, such as:

- Using backup servers, regularly backing up essential electronic files, and storing backup copies in a secure off-site location.
- Pre-positioning hard copy records to ensure an organization is not reliant on electronic equipment to access records.
- Leverage cloud computing, which disperses risk to an organization since data is not hosted on local servers.
- Raising computers above the flood level and moving them away from large windows.
- Securing equipment that could move or fall during an earthquake.
- Considering off-site protection plans such as planned dispersal, E-vaulting, or duplication of records.
- Moving heavy/ or fragile objects to low shelves;
- Purchasing fire-resistant cabinets and vaults.

Additional Suggestions

- Develop procedures to ensure staff at continuity facilities have access to appropriate media for accessing essential records as soon as possible after activation of continuity plans.
- Maintaining inventories at a number of different sites with sufficient distance away to avoid being subject to the same emergency to support continuity operations.
- Develop instructions on moving essential records (that have not been prepositioned) from the primary operating facility to the alternate site and include these instructions in the continuity plan.