Security Backup Files
as
Public Records In North Carolina:
Guidelines for the Recycling, Destruction, Erasure, and Re-use of Security Backup Files

Department of Cultural Resources
N.C. Division of Historical Resources
Archives and Records Section/Government Records Branch

Purpose: *To establish requirements under* G.S. *§ 132-3 for permitting the recycling, destruction, erasure, and re-use of security backup/data backup files and their media.*

Policy: *Security backup files are public records (according to G.S. §§ 121-2(8) and 132-1) and may not be disposed of, erased, or destroyed (according to* G.S. *§ 132-3) without specific guidance from the Department of Cultural Resources.* **These guidelines provide that guidance and permit the recycling, destruction, erasure, and re-use of security backup files and their media when an agency has implemented a written security backup plan and process that:**

- **Documents the procedures that are employed for each records series appropriate to that series' organizational value and vulnerability.**
- **Provides the minimum acceptable capability for recovery of each records series.**
- **Provides for the periodic verification that files and/or systems can be restored from the backup media as appropriate.**

Rationale for an Effective Security Backup Policy

Electronic data and information are assets. Security backups are critical to the survival of electronic data. Human or natural disasters, accidents involving the handling of media, and human error make electronic media vulnerable to damage.

"Versioning" and "Archiving" do not create security backup files. Versioning intentionally maintains copies of data files as the files are changed. Each version becomes a distinct record. Archiving is the process of moving a record from one medium (usually quickly accessible, but fragile) to another (usually more permanent) medium.

When meticulously planned and properly implemented, security backups make possible the retrieval of lost data and the resumption of system operations. Such procedures are a critical part of computer operations at all levels, especially those involving the storage of long-term or permanent records on electronic media. Security backups may also be critical to the fulfillment of audit requirements and the maintenance of audit trails in fiscal systems. For many applications, multiple copies and/or generations of backups may be recommended.

Planning and implementing security backups require consideration of several points:

Security backup files are not used as most records are. Backup files are created to protect against data loss. Backup files are typically created according to a schedule or policy; they are created, retained, and then destroyed. Security backup files provide the comfort of being able to, for a limited time, reverse an action that would normally result in the loss of a record. Backup files are created and maintained by the agency creating the original records, or by a separate agency or unit (LAN administration, information technology unit etc.) performing this service.

Security backup files are records but should always be associated with the records they serve to protect. Since electronic records must be indexed or otherwise made accessible for official use, security backup files will not normally be used to meet records retention requirements. Security backup files are generated expressly for the purpose of restoring computer systems in the event of a disaster or accidental damage. The content of security backup files may not be indexed and may not reflect the order, arrangement, or structure of the original data.

Security backup files will be found everywhere. Whether done by the originating office or by a separate unit, security backup files should be generated for all but the most transitory of records. ***Agencies are required by the Information Management Resources Commission (IRMC) to keep track of all information assets and to document the controls they have in place for safeguarding those assets***. (IRMC, "Information Asset Protection Policy", approved 5/5/98, revised 11/6/01, http://irmc.state.nc.us/documents/approvals/InformationAssetProtection.pdf).

Three factors determine the quality of a backup policy. There are three attributes that can be used to measure the quality of any system used to create and keep security backup files.

1. Persistence. This measures how well media are able to store data reliably. Every medium has an error rate; the lower this rate, the better the medium. This baseline persistence can be enhanced by creating more than one copy, keeping copies off-site or at multiple locations, media rotation, and controlling the environmental conditions.

2. Granularity. Granularity is the frequency with which backup files are made. A system in which backup files are created daily is more current than one in which backups are made weekly.

3. Duration. This is the length of time backup files are kept: specifically, the length of time after a change is made that allows that change to be reversed.

Backup policy specifications should be recorded in two ways.

1. Agencies should document the backup policies they employ or have employed for them, within the rubric of their asset protection documentation. Agencies often employ only a small number of distinct backup policies. Some record series are very important and receive the best care, while other record series are less

important and receive less care. Once a policy is established for one record series, it is often applied identically to other records with similar value. Therefore, the most efficient way to document each record series backup policy is first to describe each distinct policy and then to identify to which record series the policy applies. This kind of documentation should be a part of your agency's asset protection strategy and should be written down.

2. Each agency should establish the minimum acceptable capability for recovery that must be provided for each record series. Some record series may not warrant an explicit declaration of backup policy requirements. Agencies are, however, required to take proper care of those records that are necessary to the agency's day-to-day operations. For records that have archival, legal, fiscal, or other value that also requires longevity past the duration of the agency's normal use, the duration of the backup copies and the granularity with which they are created should reflect the requirements of those values. A system for maintaining security backup files and their associated procedures must be continued for as long as the approved retention period of the original records and data requires. Retention of security backup files for longer than the retention period specified for the original records and data may subject the agency to unnecessary risks.

For more important record series, the agency should establish specifications regarding how often copies are carried off-site, when duplicate copies must be made on-site, the type of media to use, and what provisions are in place to verify that files or entire systems can be restored from the backup media. For record series that are stored only electronically and especially for those with enduring archival, legal, fiscal, or other value, then more thorough documentation may be required in addition to the types of specifications already noted. Backup documentation should cover, among others, the elements of granularity and frequency, duplication (if applicable) and frequency, and offsite storage and frequency (how often copies---either duplicate or original security backup files---are carried offsite).

(DCR-DHR-ERTF-08/2002)