Backup, Share, And Archive Incident Data How To

Description

Backup, sharing, and archiving of incident data and project work is necessary to:

1. Minimize disruption and delay in the event of data corruption, loss, or unavailability

2. Ensure access to incident data and products

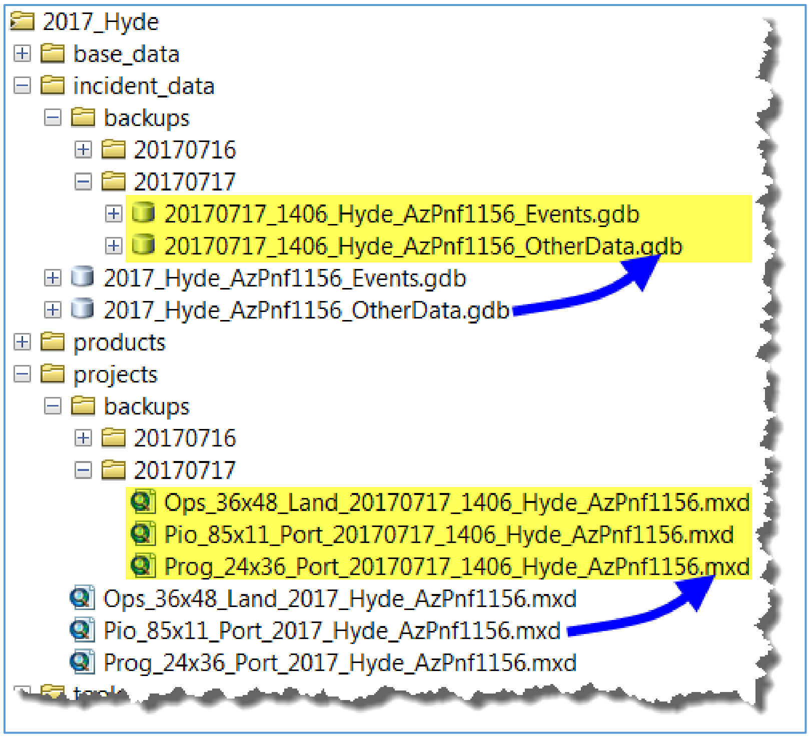
3. Ensure effective and efficient team transition

4. Preserve the incident record

Lesson Objective

Understand the three tasks necessary to backup, share, and archive incident data and projects.

GSTOP Reference – Chapter 7, *Data Sharing, Backup, and Archiving*



```
2017_Hyde
⊞ base_data
⊟ incident_data
    ⊟ backups
        ⊞ 20170716
        ⊟ 20170717
            ⊞ 20170717_1406_Hyde_AzPnf1156_Events.gdb
            ⊞ 20170717_1406_Hyde_AzPnf1156_OtherData.gdb
    ⊞ 2017_Hyde_AzPnf1156_Events.gdb
    ⊞ 2017_Hyde_AzPnf1156_OtherData.gdb
⊞ products
⊟ projects
    ⊟ backups
        ⊞ 20170716
        ⊟ 20170717
            Ops_36x48_Land_20170717_1406_Hyde_AzPnf1156.mxd
            Pio_85x11_Port_20170717_1406_Hyde_AzPnf1156.mxd
            Prog_24x36_Port_20170717_1406_Hyde_AzPnf1156.mxd
    Ops_36x48_Land_2017_Hyde_AzPnf1156.mxd
    Pio_85x11_Port_2017_Hyde_AzPnf1156.mxd
    Prog_24x36_Port_2017_Hyde_AzPnf1156.mxd
⊞ tools
```

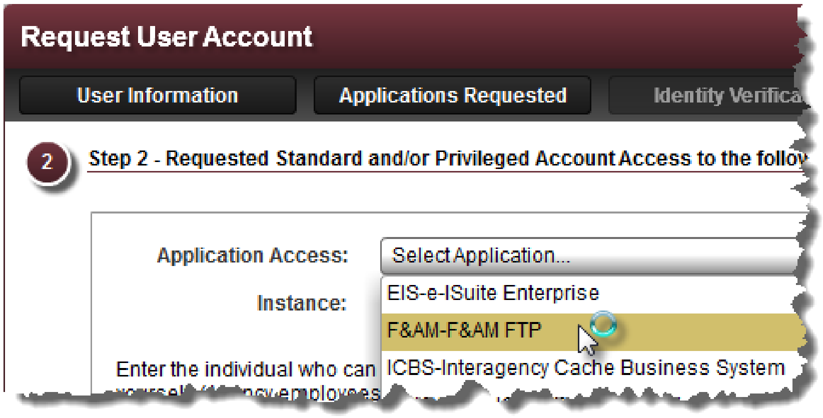
Task 1 - Backup the master incident geodatabases (MDB or GDB) and the master map documents (MXD) to a dated backup folder within the incident's local GSTOP filing structure. Do this as often as necessary, but at least once each operational period at the conclusion of that period's data edit and map update cycle.

Use either of these methods to complete this task.

1. Create dated folders within the GSTOP **incident_data\backups** folder and the **projects\backups** folder, and manually copy and rename the master incident geodatabases and the master incident MXDs using standard GSTOP file naming conventions.

2. Use the **Incident Periodic Backup** toolbox script to automatically compact, copy, and rename the master incident geodatabases and the master incident MXDs to their respective dated backup folders, as illustrated above.

Task 2 - Post the zipped incident shapefile exports (EventPolygon and EventLine), and the zipped incident Event geodatabase to a dated folder within the incident's NIFC FTP filing structure. Do this at the end of each operational period's data edit cycle.



Follow these steps to complete this task.

1. Request a **NAP** user account that has **Standard F&AM FTP** application access. Refer to the FTP NAP account guidance, and contact your FTP GACC approver to facilitate the request. This process takes some time, so do it well in advance of being on an incident.

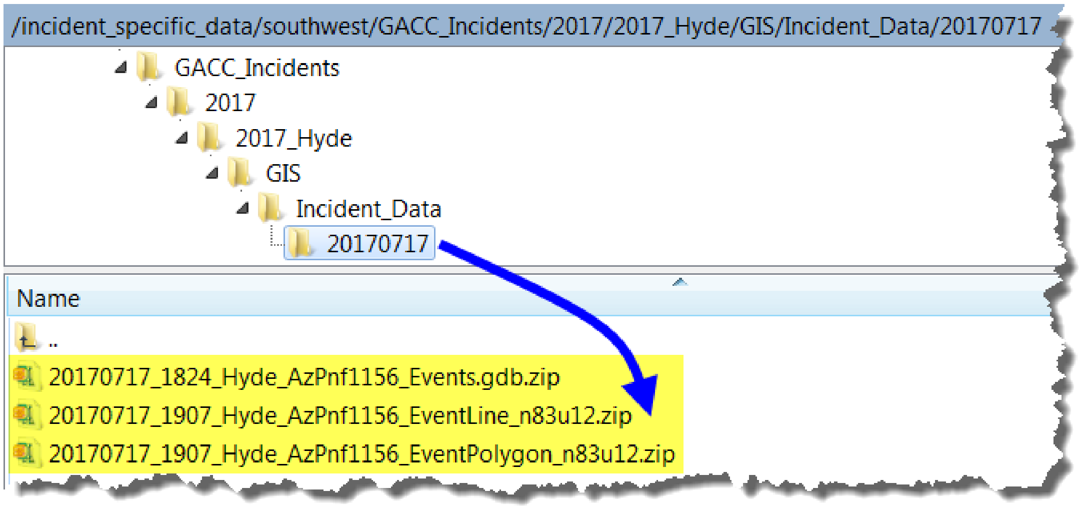
2. Install **FileZilla** or **WinSCP** FTP clients on your PC. Refer to this FileZilla link or this WinSCP link for guidance when configuring these FTP clients for use with NIFC FTP.

3. Export the incident Event geodatabase feature classes **EventLine** and **EventPolygon** to shapefile format.

4. Zip the EventLine and EventPolygon shapefile exports separately, and use FileZilla or WinSCP to post the zipped shapefiles to that period's dated FTP folder.

5. Zip the current incident Event geodatabase, and use FileZilla or WinSCP to post the zipped geodatabase to that period's dated FTP folder.

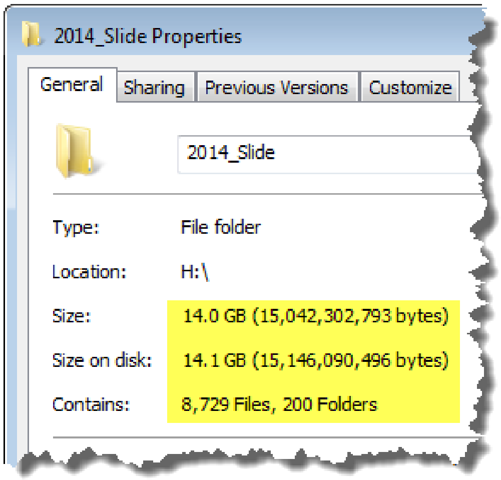
The zipped Event geodatabase and zipped shapefile exports might look something like this when posted to NIFC FTP as viewed using WinSCP.



```
/incident_specific_data/southwest/GACC_Incidents/2017/2017_Hyde/GIS/Incident_Data/20170717
GACC_Incidents
  2017
    2017_Hyde
      GIS
        Incident_Data
          20170717
Name
..
20170717_1824_Hyde_AzPnf1156_Events.gdb.zip
20170717_1907_Hyde_AzPnf1156_EventLine_n83u12.zip
20170717_1907_Hyde_AzPnf1156_EventPolygon_n83u12.zip
```

Task 3 - Archive the entirety of the incident's data, project, and product holdings to a local, off-network repository, like an external hard drive, using **Second Copy** or **RoboCopy**. Do this at least once a day.

In the example at right, the Slide fire's total holdings include 8,729 files in 200 folders, and total about 14 GB. Accumulating and preserving these data in their entirety facilitates data hand-off during team transitions, and is a critical element in documenting and maintaining an incident's GIS project record.



2014_Slide

Type: File folder

Location: H:\

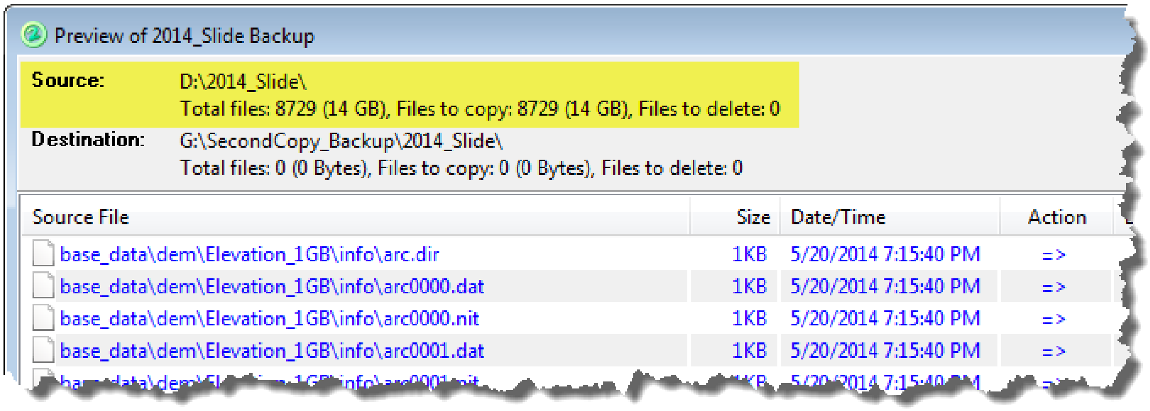
Size: 14.0 GB (15,042,302,793 bytes)

Size on disk: 14.1 GB (15,146,090,496 bytes)

Contains: 8,729 Files, 200 Folders

Listing specific steps to complete this task isn't practical because several different software and command line tools are available for use. In general, however, GISS should configure their archive routine to include these two elements.

1. The **initial archival backup** should copy the incident's entire directory tree. In this example, all 8,729 files are copied to the archive folder on an external USB drive.

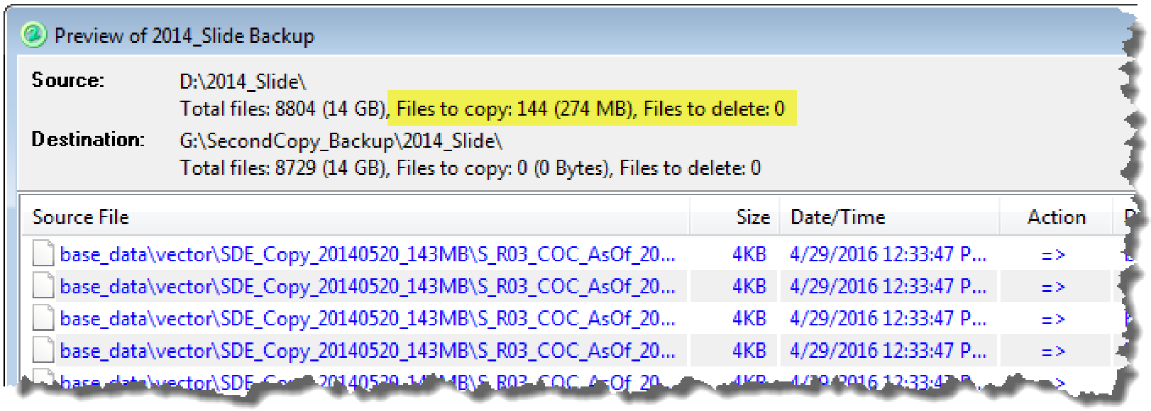


Source: D:\2014_Slide\
Total files: 8729 (14 GB), Files to copy: 8729 (14 GB), Files to delete: 0

Destination: G:\SecondCopy_Backup\2014_Slide\
Total files: 0 (0 Bytes), Files to copy: 0 (0 Bytes), Files to delete: 0

Source File	Size	Date/Time	Action
base_data\dem\Elevation_1GB\info\arc.dir	1KB	5/20/2014 7:15:40 PM	=>
base_data\dem\Elevation_1GB\info\arc0000.dat	1KB	5/20/2014 7:15:40 PM	=>
base_data\dem\Elevation_1GB\info\arc0000.nit	1KB	5/20/2014 7:15:40 PM	=>
base_data\dem\Elevation_1GB\info\arc0001.dat	1KB	5/20/2014 7:15:40 PM	=>
base_data\dem\Elevation_1GB\info\arc0001.nit	1KB	5/20/2014 7:15:40 PM	=>

2. **Subsequent archival backup** sessions should include only those files that are new, or that have been modified, since the previous archival backup. In this example, only the 144 files that have been created or modified since the last session are copied.

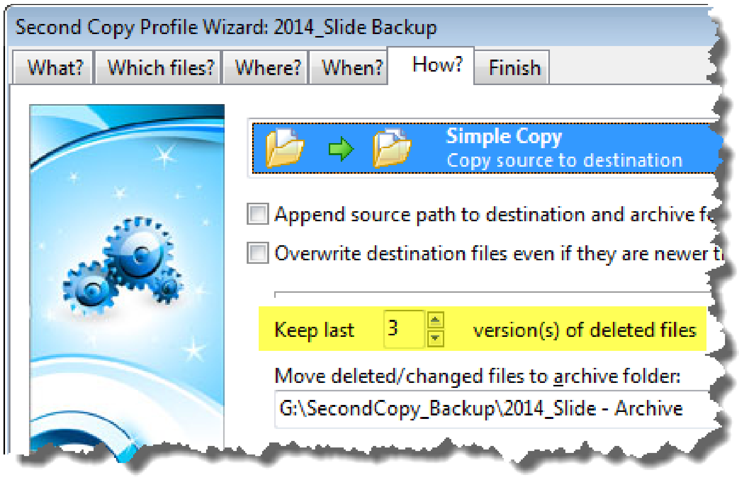


Source: D:\2014_Slide\
Total files: 8804 (14 GB), Files to copy: 144 (274 MB), Files to delete: 0

Destination: G:\SecondCopy_Backup\2014_Slide\
Total files: 8729 (14 GB), Files to copy: 0 (0 Bytes), Files to delete: 0

Source File	Size	Date/Time	Action
base_data\vector\SDE_Copy_20140520_143MB\S_R03_COC_AsOf_20...	4KB	4/29/2016 12:33:47 P...	=>
base_data\vector\SDE_Copy_20140520_143MB\S_R03_COC_AsOf_20...	4KB	4/29/2016 12:33:47 P...	=>
base_data\vector\SDE_Copy_20140520_143MB\S_R03_COC_AsOf_20...	4KB	4/29/2016 12:33:47 P...	=>
base_data\vector\SDE_Copy_20140520_143MB\S_R03_COC_AsOf_20...	4KB	4/29/2016 12:33:47 P...	=>
base_data\vector\SDE_Copy_20140520_143MB\S_R03_COC_AsOf_20...	4KB	4/29/2016 12:33:47 P...	=>

3. If possible, retain several of the most recent versions of superseded files, as in this example from Second Copy.



Second Copy Profile Wizard: 2014_Slide Backup

□ Append source path to destination and archive fo

□ Overwrite destination files even if they are newer t

Keep last 3 version(s) of deleted files

Move deleted/changed files to archive folder:
G:\SecondCopy_Backup\2014_Slide - Archive

PII and Sensitive Data – Data or products that contain personally identifiable information (PII), or that are deemed to be sensitive (cultural resources, TES species, etc.) by their originating entity are not to be posted to NIFC FTP, or to any other public-facing site. Consult with the Situation Unit Leader and with the originating entity for guidance in these situations.

Tools and References – This guidance refers to several tools or references, as described below.

- The *NWCG Standards for Geospatial Operations,* PMS 936 dated September 2014 is the primary reference for GISS practitioners. GSTOP's Chapter 2 covers file naming and directory structure. Chapter 7 covers data sharing, backup, and archiving.

- The **Incident Periodic Backup** toolbox script is available in this lesson's materials.

- The **FileZilla** and **WinSCP** FTP clients are available free from online sources.

- Simple backup software, like **Second Copy**, costs about $30.

- **RoboCopy** is a free Windows utility that facilitates creation and maintenance of an incident archive. A **RoboCopy** toolbox script is available in this lesson's materials.