



**Backup, Share,
And Archive
Incident Data**

GSTOP Chapter 7, Pages 83 - 87

Welcome to this presentation, where we'll explore the procedures to backup, share, and archive incident data.

The reference for this topic is in Chapter 7 of GSTOP, pages 83 – 87.

Lesson Objectives

- **Understand the procedures and importance of documentation, backups, data sharing, and archiving**
- **Discuss digital and hardcopy product archive requirements**
- **Review backup and archiving of the incident geodatabase**



The objectives of this presentation are to help you understand the procedures and importance of documentation, backups, data sharing, and archiving.

We'll also discuss digital and hardcopy product archive requirements,

And will review backup and archiving of the incident geodatabase.

Documentation, Backup, Data Sharing, and Archiving

- Integrate these practices into your routine
- Make it a daily habit
- Schedule time for records & data maintenance
- Will make your life easier in the end



Make documentation, backup, data sharing, and archiving a part of your routine.

Make it a daily habit to schedule time for records and data maintenance.

In the long run, good habits will save you many headaches.

Documentation

- **Standard GSTOP file naming and directory structure are designed to serve as documentation and metadata**
 - It enables easy recognition of file content
 - It facilitates archival retrieval and use
- **Use a Unit Log (ICS 214) to track significant events**



Documentation

Following standard GSTOP file naming and directory structure conventions enables easy recognition of file content by others, and serves as a form of metadata.

Use a Unit Log to:

1. Track when products are due, created, and delivered
2. Note personnel transitions and special assignments
3. Record data backup, posting, and archiving
4. Record issues or events affecting the GIS group's ability to create and deliver products

Backup

- **Data corruption and drive failures do occur**
- **Create copy of incident GDBs and MXDs at least once per operational period in the dated backup folders of the GSTOP filing structure**
- **Mirror the entire incident directory to a local off-network data storage device at least once daily to create a digital archive**



Backup

Data corruption and drive failures do occur, so backups are important!

Backups fall into two categories.

The first is to create a copy of the incident master geodatabases and master MXDs at least once per operational period in the dated backup folders of the GSTOP filing structure.

The second is to mirror the entire incident directory to a local off-network data storage device at least once daily to create a digital archive.

Data Sharing

- **Process of distributing data to authorized parties or agencies during an incident**
 - Data uploads to the NIFC FTP site
 - Incident data sharing with authorized users
 - Transfer of data at team transitions
- **Important restrictions on sharing sensitive data**
 - Cultural resources, TES species, PII, etc.
- **Check with SITL**



Data sharing is the process of distributing data to authorized parties or agencies during the course of an incident.

Three typical forms of incident data sharing are:

1. Data uploads to the NIFC FTP site
2. Incident data sharing with authorized users
3. Transfer of data at team transitions

There are important restrictions on sharing sensitive data. Sensitive data may include items like the locations of cultural resources and TES species, or data containing PII.

Check with the SITL about how, or if, to label these data on incident maps.

Maps containing these data are for incident operational purposes only, and must not be shared or posted to public-facing FTP sites or websites.

Upload Data To NIFC FTP Site

- Incident data are uploaded to the NIFC FTP site within the dated folders of the incident's filing structure
 - Zipped incident geodatabase
 - Zipped shapefiles of fire polygon and fire line layers
- This is done at the conclusion of each operational period's data edit cycle



Incident data are uploaded to the NIFC FTP site within the dated folders of the incident's filing structure.

These data include:

1. Zipped incident geodatabase
2. Zipped shapefiles of the fire polygon and fire line layers

These data should be posted at the conclusion of each operational period's data edit cycle.

Why Do We Archive?

- **Maps, part of the Permanent Incident Record**
- **Permanent records are kept at the local unit for up to 3 years, then sent to the Federal Records Center and, after 20 years, are sent to the National Archives. GIS electronic files are retained by the local unit**
- **Provides long term documentation**



Why do we archive?

Maps are part of the Permanent Incident Record that is kept in perpetuity.

Permanent records are kept at the local unit for up to 3 years, then sent to the Federal Records Center and, after 20 years, are sent to the National Archives. The GIS electronic files are retained by the local unit.

The fire incident record provides long term documentation to support management, justify funding, assess cost apportionment, support research and litigation, and facilitate planning.

Data Archiving

- **Process of moving data to a separate data storage device or media for long-term retention**
- **Mirror entire incident directory to off-network data storage device once daily**
- **Copies of the incident archive distributed to:**
 - Local Unit
 - Incident Documentation Unit



Data archiving is the process of moving data to a separate data storage device or media for long-term retention.

A digital data archive is built and maintained by mirroring the entire incident directory to an off-network data storage device on a daily basis.

Copies of the incident data archive should be made and distributed to:

1. The Local Unit
2. The Incident Documentation Unit

If sensitive data is given to you, it is not to be retained with the incident archive.

Product Archiving

- **Export a PDF of all map products to the GSTOP Products/Date folder**
- **A hardcopy of map products must printed, folded, and given to the Documentation Unit as required by archive guidelines**
- **Include Source Statement on all maps**
- **Complete feature-level metadata in GDB**



We must archive hardcopy map products, as well as digital data.

Following map export to the GSTOP Products\Date folder, a hardcopy of each map product must printed, folded, and delivered to the Documentation Unit, as required by archive guidelines.

Be sure to include a Source Statement on each map, and complete the feature-level metadata in the GDB's attribute table.

Permanent Incident Record

Maps are a part of the
Permanent
Incident Record



Documentation guidance calls for maps to be folded and boxed for inclusion in the permanent incident record.

Kind of reminds you of the last scene from Raiders of the Lost Ark! I'm just sayin'...

Remember

- In addition to making maps, your job is to leave an archived account of your work history
- Make it a part of your daily routine
- Ask SITL for additional help, if needed



Remember, in addition to making maps, your job is to leave an archived account of your work history.

Make documentation, backup, data sharing, and archiving a part of your daily routine, and it will become a habit.

If you are unable to keep up , tell the SITL that you need more help. They typically do not see these behind-the-scenes efforts, and may have little idea of the workload involved.

Review Objectives

- Understand the procedures and importance of documentation, backups, data sharing, and archiving
- Discuss digital and hardcopy product archive requirements
- Review backup and archiving of the incident geodatabase



OK, let's review.

The objectives of this presentation were to help you understand the procedures and importance of documentation, backups, data sharing, and archiving.

We also discussed digital and hardcopy product archive requirements,

And reviewed backup and archiving of the incident geodatabase.