



Standard Operating Procedure 3: Data Management

Version 1.0

Monitoring visitor use in Southwest Alaska Network



ON THE COVER

Visitors bear watching at Brooks Falls, Katmai National Park and Preserve
NPS

Standard Operating Procedure 3: Data Management Version 1.0

Monitoring visitor use in Southwest Alaska Network

Tim Shepherd, Russell Frith

National Park Service
Southwest Alaska Network
240 West 5th Avenue
Anchorage, AK 99502

August 2018

U.S. Department of the Interior
National Park Service
Southwest Alaska Network
Anchorage, Alaska

Please cite this publication as:

Shepherd, Tim, and R. Frith. 2018. Standard Operating Procedure 3: Data Management Version 1.0. Monitoring visitor use in Southwest Alaska Network. National Park Service, Anchorage, Alaska.

Contents

	Page
Figures.....	iv
Change History	1
Introduction.....	1
1. Database Design.....	3
2. System Security	3
2.1 Internet Information Services	4
2.2 Database User Schemas.....	4
3. Managing Users	5
4. Disaster Recovery and Data Retention	8
5. Sustaining Support	9
5.1 New Feature Development	9
5.2 Application Program Modifications	9
5.3 User Support.....	9
5.4 Software Upgrades	9
5.5 Server Provisioning	10
Literature.....	11

Figures

	Page
Figure 1: Stages in SWAN information technology CUA development and operations toolchain.....	2
Figure 2: CUA Visitor Use Connection String Stanza from the C#.NET Web Configuration File	4
Figure 3: Internet Information Services (IIS) Web Applications.....	4
Figure 4: CUA Visitor Use Microsoft SQL Server Visitor Use Database Schemas	5
Figure 5: Home Page of the CUA Visitor Use Data Entry Portal.....	6
Figure 6: CUA Visitor Use Web App User Access Configuration Page	7
Figure 7: CUA Data Retention and Disaster Recovery Workflow Diagram	8

Change History

Version #	Date of Revision	Revised By	Changes	Justification
1.0	08/31/2018	Shepherd	–	Original Version

This standard operating procedure (SOP) outlines methods for Commercial Use Authorization (CUA) visitor use data management. Visitor use data structures and data entry/validation workflow processes have been established by concessions working groups from Alaska park units, administrative offices, and the Inventory & Monitoring Program's Southwest Alaska Network (SWAN). This SOP describes the workflow processes needed for the implementation and support of the Visitor Use web application and database. Data management specialists are the intended audience.

Introduction

This Data Management SOP is intended to provide an overview of the database structure and other infrastructure needed to maintain the current database and web application.

SWAN information technology staff are responsible for realizing the development and operations toolchain. This toolchain is comprised of the following work categories:

- CUA coding development and review
- Building software solutions that incorporate the use of web source codes and frameworks, reporting tools, and GIS products
- Testing software deployments to assess fault tolerance and compliance with CUA business rules
- Packaging software revisions for deployment to web servers
- Releasing software maintenance builds to address system bugs, refactored interfaces, and new business requirements
- Configuring Windows Server and IIS properties
- Monitoring applications performance and end-user experiences



Figure 1: Stages in SWAN information technology CUA development and operations toolchain

In order to realize CUA operational stability, address business process revisions, and reduce risk, SWAN information technology staff engage in the following tasks:

- Configure and provide sustaining infrastructure support for the following (see SOP 3):
 - o Web server – front-end application
 - o Database server
- Build CUA web application on latest development stack
- Work with CUA web application users on maintenance items and new program functionality
- Develop and maintain database reports and views needed for annual resource briefs
- Develop database queries to address *ad hoc* inquiries
- Provide application security
- Provide disaster recovery
- Serve as a subject matter expert for business process analysis

1. Database Design

Southwest Alaska Network (SWAN) will utilize tabular data for reporting purposes. A SQL Server database managed by SWAN will be the repository for the data submitted through CUA activity reports until a national application is developed.

The database is made up of three main tables: Account Year, Trip, and Location.

The 'Account Year' table holds basic information on the report turned in by the CUA operator. This includes the company's name and CUA ID, and the reporting park. Alagnak Wild River (ALAG) locations are included in a Katmai National Park and Preserve (KATM) general report; i.e., KATM has two forms: (1) Brooks Camp and (2) KATM general, as fees for Brooks Camp are collected at a different rate than other locations in the park. There is also a field to indicate whether the company operated in the park in a given year.

The 'Trip' table is a child to 'Account Year.' The 'Trip' table holds information on trips that the CUA operator undertook. The table holds a trip's start and end dates, number of clients, number of guides, and whether the trip was an unguided drop-off.

The 'Location' table is a child to 'Trip.' The 'Location' table holds the location name (visitor use monitoring area), primary activity for the location, and visitor use days (the total number of people multiplied by the number of days at location).

The database also has a number of tables that hold lookup/fixed values that are used to control data entry and reduce data entry errors.

The CUA table holds information on the companies with a CUA permit. The table contains the assigned CUA ID, which is an administrative identifier assigned by the Regional Concessions Office. The table also holds the company's name. The CUA ID is part of the Account Year record as a foreign key.

The Activity table contains the list of activities and associated codes (code are set by the regional office). The activity field is included in the Location table as a foreign key. Allowed activities vary by park.

The Location table holds the names for the Visitor Use Monitoring Areas. The location name is part of the Location table and is included as a foreign key.

2. System Security

The system security of the Visitor Use web application builds on existing agency information technology security implementations and policy. The system security implementation is a best practices solution derived from guidance provided in personnel training modules referenced in Section 6.3 of the Visitor Use Protocol narrative.

2.1 Internet Information Services

The internet information services (IIS) security policy allows users with DOI Active Directory Service user accounts to pose database queries to the Visitor Use database. This IIS policy is programmed into the Visitor Use web application *web.config* resource file.

```
<connectionStrings>
  <add name="SWANVisitorUseConnectionStringOld" connectionString="Data Source=
;Initial Catalog=
;Integrated Security=True" providerName="System.Data.SqlClient"/>
  <add name="SWANVisitorUseConnectionString" connectionString="Data Source=
;Initial Catalog=
;Integrated Security=True" providerName="System.Data.SqlClient"/>
  <add name="SWANVisitorUseConnectionString1" connectionString="Data Source=
;Initial Catalog=
;Integrated Security=True" providerName="System.Data.SqlClient"/>
</connectionStrings>
```

Figure 2: CUA Visitor Use Connection String Stanza from the C#.NET Web Configuration File

The “integrated security” option of the connection string instructs IIS to permit only users with DOI active directory service accounts the rights to query the Visitor Use database. Subsequent application restrictions may prohibit users from doing this. See Section 3. The configuration parameters for IIS are show in the figure below.

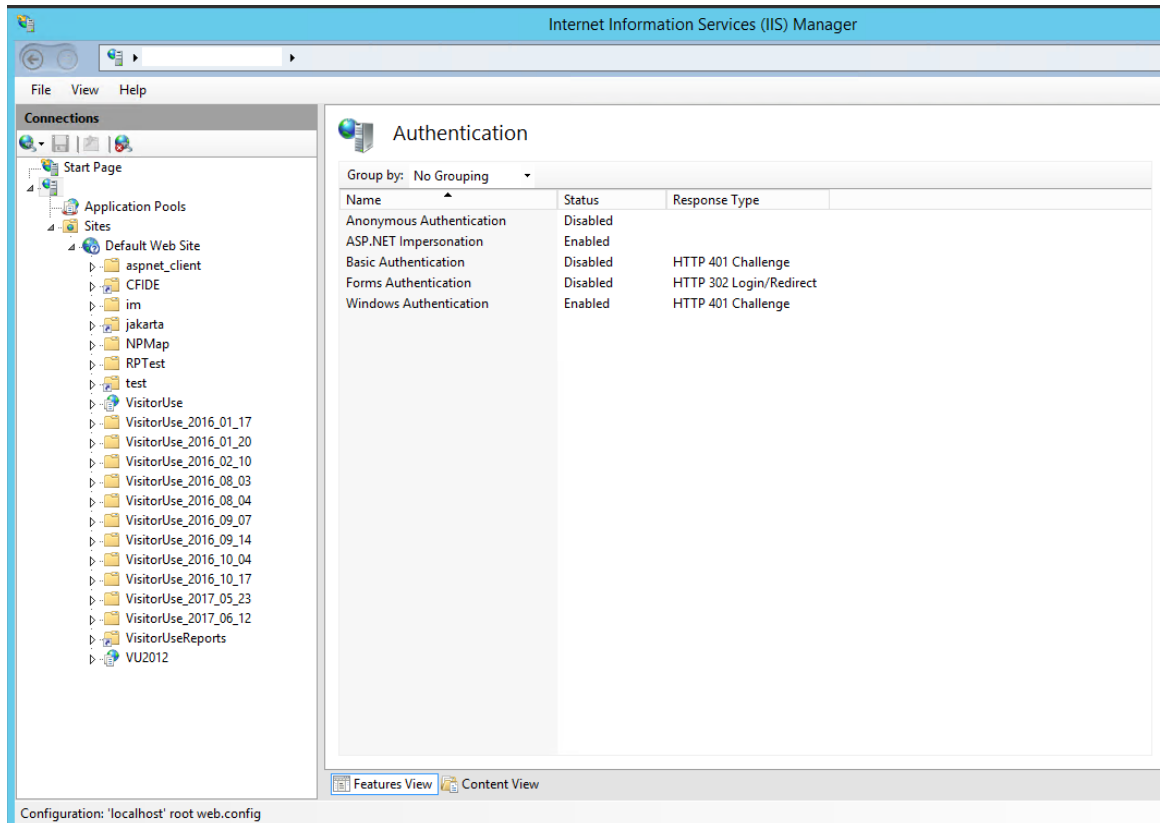


Figure 3: Internet Information Services (IIS) Web Applications

2.2 Database User Schemas

The Visitor Use database is accessed using the NT AUTHORITY\ANONYMOUS LOGON credential when a database operation is received from IIS.

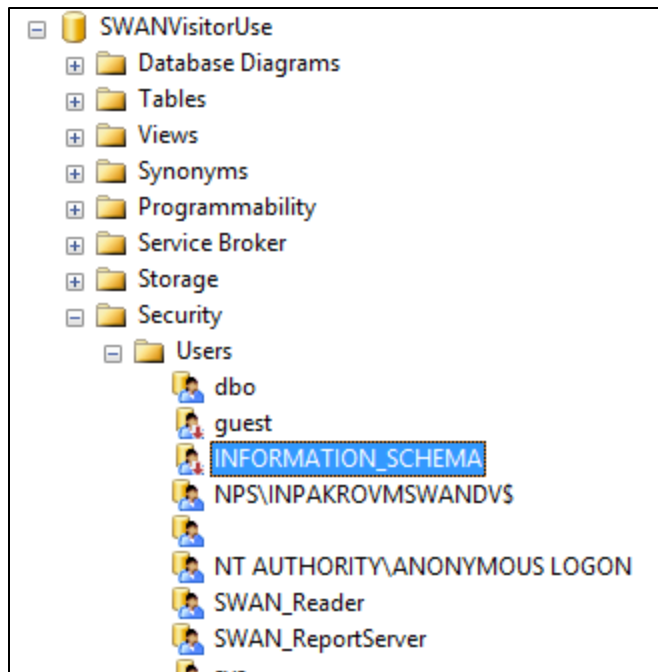


Figure 4: CUA Visitor Use Microsoft SQL Server Visitor Use Database Schemas

3. Managing Users

The SWAN Visitor Use web application supports an interface for adding authorized users and removing users. The user management interface provides SWAN data manages the ability to assign data view and edit privileges. Data edit privileges are required if a user is loading data into the Visitor Use database. The user management interface is on the home page of the Visitor Use web portal, as shown in the figure below.



NATIONAL PARK SERVICE

Southwest Alaska Network Inventory and Monitoring

Visitor Use Monitoring

Commercial Use Authorization (CUA) Activity Report

[NPS - Commercial Use Authorizations Page](#)

Users' Guide (*Under Construction*)

Enter and View CUA Activity Reports

Select a CUA

4 Seasons Vacations | CUA2032 | Inactive

▼

Enter

View, Enter New, or Update CUA Activity Reports by Selected CUA ID or Name

Import Data Directly from Excel

View by Name

View by ID

Your Identity Is: NPS\RGFrith

Your Role Is:Admin

Resource Briefs

[Spatial Query \(New\)](#)

[Visitor Use Counts in Lake Clark by Year & Select Location](#)

[Visitor Use Counts in Lake Clark by Year & Month](#)

[Visitor Use Counts in Lake Clark by Year & Activity](#)

User Administration

[Manage Users](#)

Figure 5: Home Page of the CUA Visitor Use Data Entry Portal

The user management interface is accessed by clicking on the link “Manage Users.” This action results in the user management page being displayed as shown in the figure below.

[Back to Menu](#)

	User Name	Role Name	Photo
Edit Delete New		Select a role Admin DataEntry DataViewer	DataEntry
Edit Delete New		Select a role	DataViewer
Edit Delete New		Select a role	DataEntry
Edit Delete New		Select a role	Admin

12

Figure 6: CUA Visitor Use Web App User Access Configuration Page

From this interface, users can be granted permission to view and/or edit the data in the database. The user name is the user's DOI Active Directory logon identifier. The following user roles are defined for granting permission:

- Admin: Users with this role can view, insert, update, and delete data in the SWAN Visitor Use database. They also have the ability to add users and change their permission level.
- Data Entry: Users with this role can view, insert, and update data in the SWAN Visitor Use database.
- Data Viewer: Users with this role can only view data from the SWAN Visitor Use database.

All users are able to run and view reports that are defined in the Visitor Use web application.

4. Disaster Recovery and Data Retention

The CUA Visitor Use database is a time series accounting of public utilization of the parks. As with all electronic storage systems, the database storage solution is vulnerable to failure. To defend against failure vulnerabilities, guidance is provided in mandated training for data managers. The required training regimen is listed in Section 5.3 of the Visitor Use Protocol Narrative. SWAN data management has leveraged that guidance to provide a best-practices solution for addressing matters of disaster recovery and data retention. The daily backup procedure and data retention policy are depicted in the following process diagram.

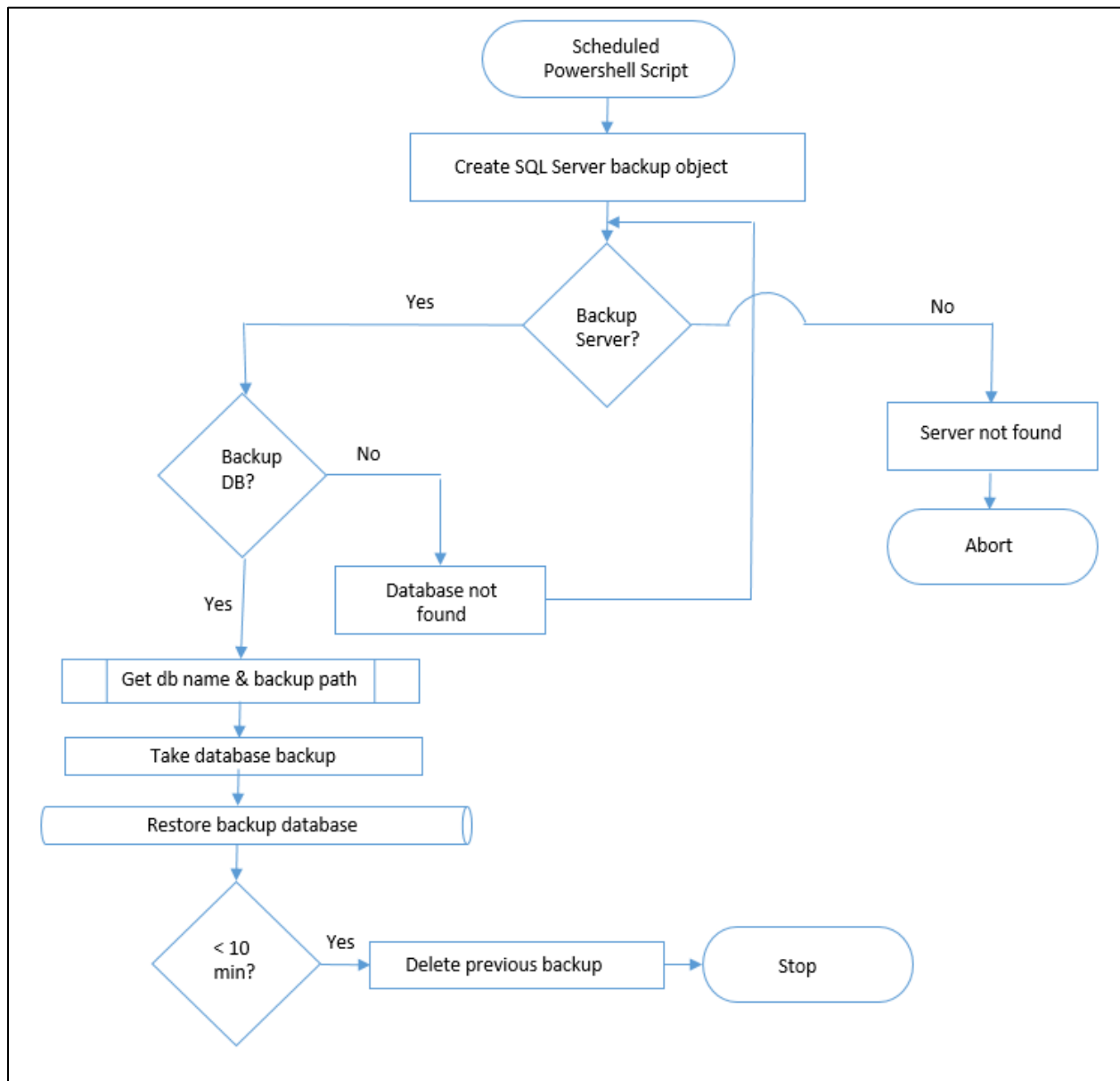


Figure 7: CUA Data Retention and Disaster Recovery Workflow Diagram

5. Sustaining Support

The CUA Visitor Use software system is an enterprise application that supports concessions management operations and park decision making. Sustaining support consists of information technology tasks that contribute to visitor use data acquisition, data storage, and data analysis. The software applications and database are realizations of conceptual business processes defined by the regional office concessions group. SWAN data managers must function as subject matter experts on the rules and policies that govern visitor use business processes in order to provision the technology solutions that make enterprise applications work. The workings of the enterprise application consist of development tasks and operations tasks, referred to as “DevOps.” These tasks are described below.

5.1 New Feature Development

The Visitor Use web application interface has to be general and extensible in order to provide efficient service delivery for a community of users who typically engage the application only once during an end-of-season data loading event. SWAN data management are tasked with constructing an intuitive, easy-to-use interface that accommodates a variety of user experience expectations. The requirements of such tasks are gathered from informal, agile user requests and assessed for inclusion into the application interface. Once a new feature request is vetted, that feature is implemented using a combination of resources referenced in Section 6.3 of the Visitor Use Protocol Narrative.

5.2 Application Program Modifications

Due to the integrated, distributed, data-driven construction of the visitor use web application, vulnerabilities exist that have the potential to impede system operations and/or produce incorrect results. SWAN data management is tasked with identifying and mitigating issues arising from, and controlling for, those vulnerabilities. Such vulnerabilities are distributed in three areas that include source code for the visitor use application, the database management system, and the internet backplane. The vulnerabilities are manifested in the forms of both software and hardware constructs.

5.3 User Support

In order to meet operational expectations of the visitor use application stack, SWAN data management has to possess a proficiency facility of the visitor use business process. The data cycle of the business process is modeled in the underlying visitor use data store and is elaborated on in Section 1, “Database Design,” of this document. SWAN data management is tasked with being subject matter experts in the mapping of the relational database structure to the web user interface. This requirement facilitates the abstraction of the underlying database architecture and serves to isolate the data store from ad hoc user engagements with the user interface. This requirement also contributes to a need to support user operations.

5.4 Software Upgrades

The operating system, software, and database stacks that comprise the visitor use application are not immutable and are subject to frequent upgrades, design paradigm shifts, and patches. These external events pose challenges to sustaining long-term operations of the application. As such, data management is tasked with retaining operational consistency across periodic stack modifications.

Those tasks require intervening application development of the web and database components as well as intervening responses to system configuration changes.

5.5 Server Provisioning

The information technology backplane of the visitor use application consists of a web server (distributed, server-side operating system) and a database server. The web server is configured to allow simultaneous, multiple client data operations to securely interact with the server-side database. The web-server serializes user data service requests using a first-come, first-served protocol. The database server is configured to provide vetted user access to the visitor use database. Database management constructs user schemas that regulate user rights to view and edit data.

Literature

This standard operating procedure was written in support of the visitor use protocol.

Shepherd, T. and R. Frith. 2018. Monitoring visit use in the Southwest Alaska Network using Commercial Use Authorization (CUA) Reports. Natural Resource Report NPS/SWAN/NRR—2018/1693. National Park Service, Fort Collins, Colorado.

The Department of the Interior protects and manages the nation's natural resources and cultural heritage; provides scientific and other information about those resources; and honors its special responsibilities to American Indians, Alaska Natives, and affiliated Island Communities.

August 2018

National Park Service
U.S. Department of the Interior

