Stantec

DATA MANAGEMENT ANALYSIS & RECOMMENDATION REPORT

December 29, 2023

Prepared for:
Port Gamble S'Klallam Tribe

Prepared by:
Stantec | Digital Technology & Innovation

Revision	Description	Author	Date	Quality Check	Date
1.0	New Document	Himanshu Saluja, Ross Poulin	12/13/2023	Ashwini Shankar	12/15/2023

The conclusions in the Report titled Data Management Analysis & Recommendation Report are Stantec's professional opinion, as of the time of the Report, and concerning the scope described in the Report. The opinions in the document are based on conditions and information existing at the time the scope of work was conducted and do not take into account any subsequent changes. The Report relates solely to the specific project for which Stantec was retained and the stated purpose for which the Report was prepared. The Report is not to be used or relied on for any variation or extension of the project, or for any other project or purpose, and any unauthorized use or reliance is at the recipient's own risk.

Stantec has assumed all information received from Port Gamble S'Klallam Tribe (the "Client") and third parties in the preparation of the Report to be correct. While Stantec has exercised a customary level of judgment or due diligence in the use of such information, Stantec assumes no responsibility for the consequences of any error or omission contained therein.

This Report is intended solely for use by the Client in accordance with Stantec's contract with the Client. While the Report may be provided by the Client to applicable authorities having jurisdiction and to other third parties in connection with the project, Stantec disclaims any legal duty based upon warranty, reliance or any other theory to any third party, and will not be liable to such third party for any damages or losses of any kind that may result.

Prepared by: Himanshu Saluja
Signature

Himanshu Saluja
Printed Name

Reviewed by: Ashwini Shankar
Signature

Ashwini Shankar
Printed Name

Approved by: Poulin, Ross
Digitally signed by Poulin, Ross
Date: 2023.12.29 13:33:45 -07'00'
Signature

Ross Poulin
Printed Name

Table of Contents

1 Introduction

Stantec has been commissioned by the Port Gamble S'Klallam Tribe (PGST) Natural Resource Department (NRD) to assess their existing data management practices and develop a Data Management Plan to drive consistency and incorporate best practices in the delivery and execution of their projects.

On-site workshops and stakeholder interviews provided valuable insight and understanding in current data management methods, processes, and tools utilized by PGST teams to deliver their work. This document outlines our methodology, provides recommendations and best practices on areas for improvement as it relates to file naming convention, version control, use of keywords and metadata, document control processes, and archival.

The Document Management Plan establishes the framework and processes to support document management within the PGST program by standardizing the filing system for all program- and project-level documents. It outlines the appropriate procedures to be followed so that documents are organized and maintained correctly. Document management fulfills the critical function of maintaining an official record of activities associated with the program.

2 Objective

The objective of this Recommendation Report is to develop a comprehensive Data Management Plan for the Port Gamble S'Klallam Tribe's Natural Resources Department.

The plan aims to:

- Establish best practices and consistency in data management.
- Improve document control.
- Enhance the utilization of Microsoft 365, OneDrive, Outlook, and Natural Resources Server.

It also guides the organization in effective file naming conventions, version control, keyword usage, metadata implementation, document control processes, and archival, as well as seamless integration with geospatial and mapping best practices.

3 Project Initiation

Project initiation is the first phase of a project's life cycle and involves defining the project, establishing its objectives, and determining the best approach to achieve those objectives. This phase is critical to the success of the project, as it sets the foundation for all subsequent phases. During project initiation, key stakeholders were identified, and project requirements were outlined defining the scope, goals, deliverables, and timeline of the project.

Following the kickoff call, Stantec collaborated with identified PGST stakeholders in the development of a data management plan for the delivery and execution of projects by internal and external stakeholders.

4 Current State Assessment

4.1 Interviews - Observations and Impacts

The observations made during the interviews and the impact they have on the team are as follows:

Category	Observation	Impact
Data Storage and Accessibility	Lack of a centralized file repository or universal shared repository for data storage and access.	Teams manage data independently, leading to inefficiencies in data retrieval, exchange, and access rights management.
Naming Conventions	Absence of standardized naming conventions for files.	Hindrance in data organization and retrieval.
Data Sources and Formats	Varied data sources and formats, including data from sensors and manual collection.	Inconsistencies in data format and digitization processes.
Data Storage Locations	Data stored in diverse locations, including private iCloud, external drives, and home locations.	Increased risk of data loss, accessibility issues, and lack of centralized control.
File Formats	Different departments using various file formats, with Excel being the predominant choice.	Diverse file formats may pose challenges in data interoperability.
Reporting Tools and Licenses	Some teams using FileMaker Pro for reporting with limited licenses.	Limited access to reporting tools may hinder efficient data analysis.
Data Input	Majority of data received through paper forms.	Manual data entry may result in errors and delays.
Data Security	Lack of data security measures; folders and files open across the department.	Increased risk of unauthorized access and data breaches.
Retention and Archival Policy	Lack of data retention and archival policy leading to increased server and physical storage needs.	Inefficient use of storage resources and potential compliance issues.

Category	Observation	Impact
Training and Standard Operating Procedures (SOPs)	No SOPs or training materials due to low staff turnover.	Potential knowledge gaps and lack of standardized procedures.
Data Accuracy and Investigation Procedures	Data accuracy maintained based on trust, lacking investigation procedures for inaccuracies.	Risk of relying on inaccurate data without a systematic correction process.
Data Sharing and Version Control	Data sharing through email and OneDrive, lacking version control mechanisms.	Challenges in maintaining the latest version and avoiding data duplications.

4.2 Challenges and Pain Points

The teams are facing the following challenges:

- **Lack of Centralized Data Repository**: Absence of a department-wide file repository or universal shared repository. Teams manage data independently, leading to inefficiencies in storage, access, and data exchange.

- **No Standard Naming Conventions**: Lack of standardized naming conventions for files, leading to difficulty in organizing and retrieving data and lack of consistency and confusion in data management.

- **Diverse Data Sources and Formats**: Varied data sources and formats, including sensor data and manual collection, leading to inconsistencies in data format and digitization processes.

- **Weather Constraints in Data Collection**: Weather constraints, especially rain, affecting digital data collection, leading to incomplete or inaccurate data entered during adverse weather conditions.

- **Image Data Management**: Some teams are storing image data in private iCloud or external drives, leading to increased risk of data loss, accessibility issues, and lack of centralized control.

- **Diverse File Format**: Different departments using various file formats, despite Microsoft Excel as the predominant tool leads to potential challenges in data interoperability.

- **Limited FileMaker Pro Licenses**: Limited licenses for FileMaker Pro, hindering widespread use for reporting. Therefore, restricted access to reporting tools, limiting data analysis to Excel.

- **Data Collection Dominated by Paper Forms**: Majority of data collection is happening through paper forms, leading to manual data entry introducing delays.

- **Server and Physical Storage Challenges**: Lack of data retention and archival policy leading to increased server and physical storage needs which in turn leads to inefficient use of storage resources and potential compliance issues.

- **Data Security and Access Control**: Lack of data security measures; folders and files open across departments, leading to increased risk of unauthorized access and data breaches.
- **Standard Operating Procedures (SOPs) and Training Gaps**: No SOPs or training materials due to low staff turnover might lead to potential knowledge gaps and lack of standardized procedures.
- **Absence of Data Accuracy Investigation Procedures**: Data accuracy maintained based on trust, lacking investigation procedures for inaccuracies which in turn leads to risk of relying on inaccurate data without a systematic correction process.
- **Email and OneDrive Data Sharing Challenges**: Data sharing mostly through email or OneDrive, involving challenges in version control and permissions. Therefore, difficulty in keeping the latest version, leading to data redundancy.

4.3 Preferences and Priorities

- Unknown

4.4 Personas/Users

The following teams were involved during the interviews:

- Administration Team
- Enhanced Program Team
- Environmental Program Team
- Finfish Program Team
- Forest & Conservation Program Team
- Research & Monitoring Program Team
- Shellfish Program Team
- Wildlife Program Team
- IT Team

5 Guiding Principles

In the development of the document control strategy, there are four guiding principles. The principles outlined below serve as the basis for system creation.

1. **Where possible, obtain and maintain documents electronically.** Contracts and agreements with consultants, contractors, and suppliers should stipulate that document—when feasible—be delivered electronically.

2. **Limit duplicate copies.** Multiple copies of documents should be minimized. In rare instances, there may be a need to locate a document in more than one place within the Document Management System (DMS). If necessary, a link to the document in the system of record should be used rather than a copy of the document created.

3. **Track decision-based documents.** Any document that contains a decision related to the program or individual project should be maintained in the document repository. Decisions should also be tracked using a Decision/Action Log.

4. **Shared drives should be used sparingly.** The shared drive should not be used to store program or work project-specific documentation. Shared drives may be applicable for very large files and their use will be determined on a case-by-case basis as the need arises. Local hard drives (e.g., C drive, My Documents), private network drives, and any other media that are not secure or backed up on a regular basis are not appropriate repositories for PGST Program electronic documents.

6 Roles and Responsibilities

Document management is the responsibility of all PGST NRD Program staff. The responsibility for maintaining and enforcing compliance with document management procedures lies with the PGST NRD Administrators with support from the Document Manager as follows.

Role	Responsibilities
PGST Program Administrator (SharePoint Administrator on Program Team)	• Establishes and maintains document management policy. • Provides periodic system status and enhancement requests to PGST management. • Monitors project document repositories, systems, and tools. • Manages user access to the DMS systems.
Document Manager	• Performs quality control and quality assurance (QA/QC) of program management documents and document management procedures. • Maintains the Document Management Plan. • Monitors document repositories (SharePoint, network share, hardcopy files) to verify that documents are filed correctly and notifies the project manager of any inconsistencies. • Manages and controls the various document processes and logs (either spreadsheets or within SharePoint) for the PGST Program Team. • Provides guidance and training on document control processes to the PGST Program Team. • Performs quality reviews to verify that documents are filed in accordance with the established document control conventions and processes. • Addresses questions/issues from end users. • Manages final and published documents as PGST Program records in accordance with business, legal and regulatory requirements. • Routinely encourages and enforces compliance among PGST Program staff with the document management procedures and systems requirements. • Defines and communicates detailed document management procedures, as needed. • Assists Program staff with document management including filing documents to program or project documents library. • Distributes received documents, as required. • Manages the control and maintenance of received hard copy documents.

7 Recommendation

The recommendations based on the interviews are as follows:

7.1 File Repository and Data Access

7.1.1 Establish a Centralized Data Repository

Current State	The absence of a centralized data repository leads to data silos and hinders collaboration.
Recommendation	Implement a centralized data repository accessible to all teams, ensuring a universal location for storing, accessing, and exchanging data. Implementing a centralized data repository involves choosing an appropriate platform and configuring it to meet the specific needs of PGST. In this case, considering the requirements and common practices, ***Microsoft SharePoint*** is recommended as the platform for the centralized data repository. Microsoft SharePoint is a widely used collaboration platform that facilitates the creation of intranet sites for document management and storage. It provides robust features for version control, access management, and collaboration, making it suitable for PGST's requirements. SharePoint is implemented at PGST to provide a collaboration area for PGST Program staff and project teams. It serves as a repository for program/project documents/deliverables for working/final documents and reference material for project teams. In addition, it will serve as the platform for project/program reporting and performance tracking. While the PGST environment is used for a variety of functions, only the functionality associated with document management is discussed within this plan. In addition to establishing a centralized document repository, it is recommended to share documents via URLs, especially for those requiring action from stakeholders. Instead of the traditional method of downloading the file, attaching it to an email, and requesting the recipient to download, it is more efficient to share the URL of the document. This allows the recipient to take the necessary action on the central repository site and enables all authorized individuals to track changes in the document. This approach not only minimizes document redundancies but also ensures the integrity of the latest version.
Example	Utilize Microsoft SharePoint as a centralized repository, creating department-specific folders with defined access controls and granting permissions based on job roles to ensure data security.

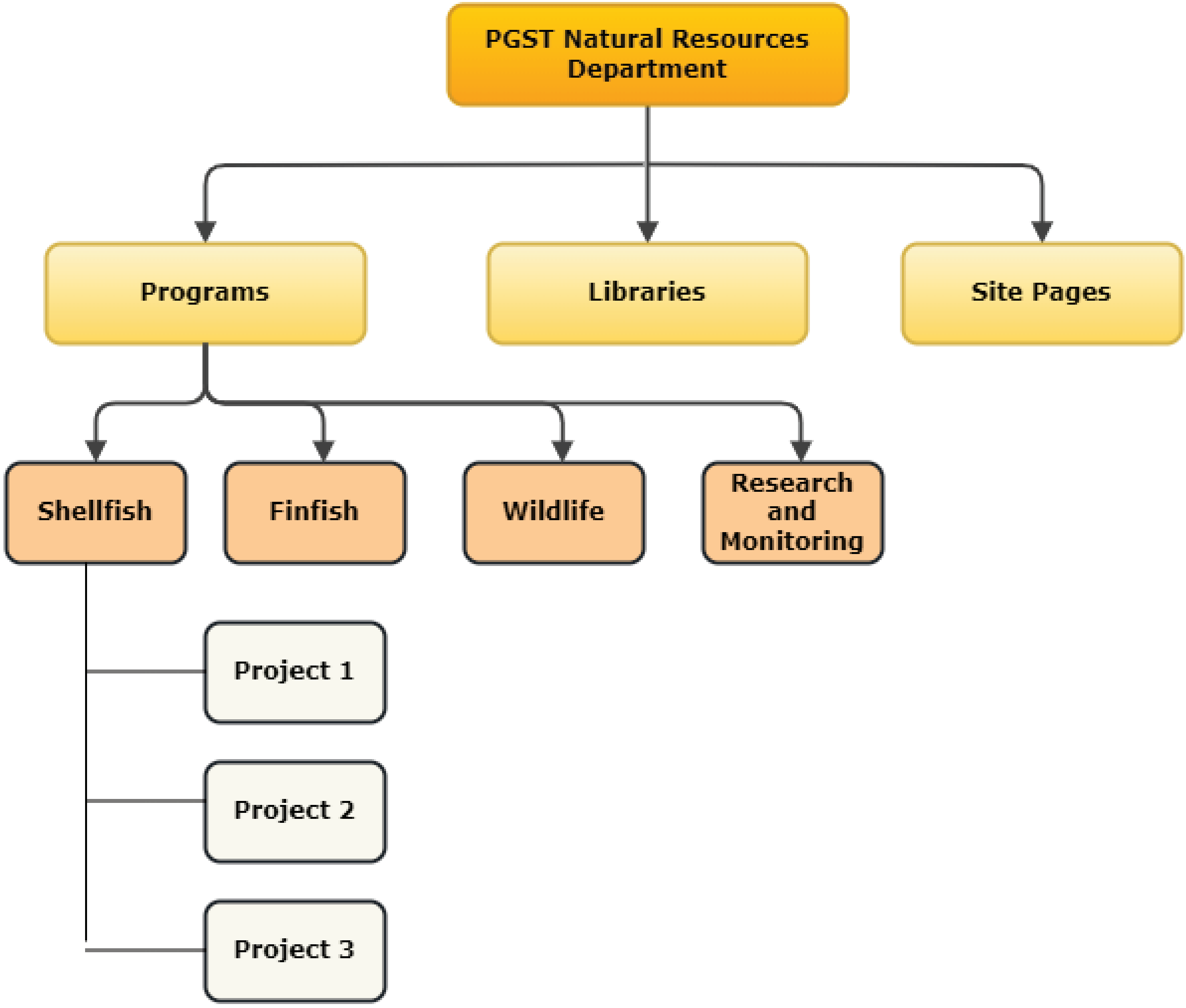
Here are a few alternatives to SharePoint for implementing a centralized data repository:

- **Google Workspace (formerly G Suite)**
  - **Why**: Google Workspace offers Google Drive, a cloud-based storage solution with collaboration features. It provides real-time collaboration on documents and easy sharing.
  - **How**: Create dedicated folders for each department and project within Google Drive. Define access permissions and organize files accordingly. Teams can collaborate on Google Docs, Google Sheets, and Google Slides.

- **Dropbox Business**
    - **Why**: Dropbox Business is a cloud-based file storage solution designed for teams. It allows secure file sharing and collaboration.
    - **How**: Set up dedicated team folders and subfolders within Dropbox. Define access controls and permissions. Teams can collaborate on files within the Dropbox platform.
- **Box**
    - **Why**: Box is a cloud-based content management platform with robust collaboration features. It is designed for secure file sharing and collaboration.
    - **How**: Create dedicated folders and workspaces within Box for each department. Customize access controls and permissions. Teams can collaborate on documents, store files securely, and maintain version history.
- **Confluence by Atlassian**
    - **Why**: Confluence is a team collaboration platform that allows creation and sharing of documents, pages, and multimedia content.
    - **How**: Create dedicated spaces for each department and projects within Confluence. Teams can collaborate on pages, upload documents, and organize content hierarchically.

7.1.2 Folder Repository Structure

Current State	Lack of centralized program/project repository structure.
Recommendation	A well-organized SharePoint document repository involves creating a clear hierarchy using libraries, folders, and projects, while also considering the use of content types, views, and information architecture to ensure an efficient and user-friendly document management system.
Example	Below diagram shows the basic structure.



7.1.3 Implement Access Control Policies

Current State	Lack of access control on data leads to security risks and compromises confidentiality.
Recommendation	Define and implement access control policies to restrict data access based on roles and responsibilities of individuals or groups within PGST. Defining and implementing access control policies is crucial for ensuring the security and confidentiality of data within a centralized repository.
Example	Assign read-only access to certain teams and grant full access to specific individuals based on their job functions. This ensures that sensitive data is only accessible to authorized personnel, enhancing data security.

How to define and implement access control policies?

- Identify User Roles: Identify different roles within PGST that require access to the centralized data repository. Common roles may include administrators, managers, team members, and external collaborators.

- Define Access Levels: Clearly define the access levels associated with each role. Access levels can include read-only, edit, delete, and administrative privileges. Tailor access levels to align with the responsibilities of each role.

- Map Roles to Data Categories: Identify the categories or types of data stored in the repository. Map each user role to the specific data categories they should have access to based on their job responsibilities.

- Consider Need-to-Know Principles: Adhere to the "need-to-know" principle, ensuring that individuals only have access to the data necessary for them to perform their job functions. Avoid unnecessary exposure of sensitive information.

- Define Exceptions and Special Cases: Identify any exceptions or special cases where individuals may need elevated access for specific tasks. Clearly document and manage these exceptions to maintain a secure access environment.

Implement Access Control Policies

- Access Control Lists (ACLs): Leverage access control lists to assign specific permissions to users or groups. ACLs allow administrators to specify who can access, modify, or delete data within the repository.

- Role-Based Access Control (RBAC): Implement role-based access control to streamline the assignment of permissions. Assign users to predefined roles and grant appropriate permissions to those roles.

- Authentication Mechanisms: Implement strong authentication mechanisms to ensure that users are who they claim to be. This may include password policies, multi-factor authentication, and integration with identity management systems.

- Regularly Review and Update Access Permissions: Conduct regular reviews of access permissions to ensure they align with current roles and responsibilities. Update permissions promptly when job roles change or when individuals no longer require access.
- Audit Trails: Enable audit trails or logs to track user activity within the repository. Regularly review these logs to detect and investigate any unauthorized access or suspicious activities.
- Document Access Control Policies: Clearly document access control policies in an accessible and comprehensive document. Ensure that all users are aware of these policies and have access to the guidelines.
- Communication: Communicate any changes to access control policies promptly. Inform users about updates, new roles, or modifications to permissions to maintain transparency.
- Periodic Access Reviews: Conduct periodic access reviews to validate that individuals still require access to their assigned data categories. Remove access for individuals who no longer need it.
- Incident Response Plan: Develop an incident response plan to address and mitigate any security incidents related to unauthorized access. Clearly outline the steps to take in the event of a security breach.

7.2 File Naming Conventions and Standardization

7.2.1 Standardize File Naming Conventions

Current State	Inconsistent file naming conventions lead to confusion and inefficiencies.
Recommendation	Establish a standardized file naming convention across all teams to enhance organization and retrieval of files. A consistent naming convention makes it easier to locate and understand files, improving overall efficiency. A standardized convention is used for both program- and project-level documents. Electronic documents are named by members of the PGST Program Team, document owners and others, using the approved document naming convention that concatenates the appropriate program/project short name, a short descriptive name of the document, and when applicable a date (YYYYMMDD), with underscores separating the components. Information such as version number, editor/author's name, is automatically captured by SharePoint in the document version history and should not be included in the name or title of the document. Adding this information to the document name will result in multiple copies of the same document being loaded into the Data Management System (DMS). This type of information will be captured in document property fields, or metadata, that will be associated with each document when it is uploaded into the DMS. If a user is unsure of how to name a document, they should contact the Document Manager assigned to the PGST Program. Here is the recommended format for the program level documents: *[DATE]_ProgName_[ProjectName]_[DESCRIPTION]* Example: *20222707_ShellFish_Grants_MeetingNotes* ***Note:*** If a single document applies to more than one project, users should consider it a program level document. In rare cases where a document clearly is associated with more than one project and should not be considered a program-level document, it may be acceptable to place the document in both project libraries. In these cases, your assigned Document Manager should be consulted before proceeding.
Example	Adopt a naming convention, such as "ProjectName_Date_Type" for uniformity and clarity. Here is the simple example for a project-related document: Project Name: Finfish_Project Date: YYYYMMDD (e.g., 20231119 for November 19, 2023) Document Type: Report, MeetingMinutes, Presentation Combined Example: Finfish_Project_20231119_Report.docx

How to define the Standardized File Naming Convention?

- Identify Key Elements: Determine the key elements that should be included in the file names. Common elements include project name, date, document type, or any other relevant identifier.
- Sequence and Order: Define the sequence and order of the elements within the file name. For example, the project name might come first, followed by the date and document type.
- Use of Delimiters: Choose delimiters (characters to separate elements) that are easily readable and do not conflict with common file naming conventions. Underscores (_), hyphens (-), or spaces () are commonly used.

- Character Limit: Consider any character limits imposed by the file system. Ensure that the chosen file naming convention complies with these limits to prevent issues with file storage and retrieval.
- Avoid Special Characters: Avoid using special characters that might cause compatibility issues with different operating systems or applications. Adhere to alphanumeric characters and commonly accepted symbols.
- Include Version Information (if applicable): If versioning is a consideration, decide whether version information should be included in the file name and establish a consistent format (e.g., v1, v2, Rev1, Rev2).
- Document the Naming Convention: Clearly document the standardized file naming convention in a guide or document that is easily accessible to all team members. This document should serve as a reference for consistent file naming practices.

7.3 Data Collection Methods and Formats

7.3.1 Promote Digital Data Collection

Current State	Varied data collection methods, including paper forms, result in inefficiencies and potential errors.
Recommendation	Encourage teams to adopt digital data collection methods to improve accuracy, streamline processes, and enhance data accessibility. When collecting data via paper methods and hard copies are unavoidable, it is advisable to scan the documents on the same day and convert them into a digital format with an appropriate naming convention. Subsequently, the digitalized data should be placed in the correct document repository structure. This practice ensures the preservation and organization of the data for easy access and retrieval. Additionally, it reduces the risk of loss or damage associated with physical documents.
Example	Implement mobile data collection apps that function offline and allow teams to collect real-time data even in adverse weather conditions, ensuring timely and accurate data entry. This eliminates the need for manual data entry and reduces the risk of errors.

The benefits of promoting digital data collection methods are as follows:

- Improved Accuracy: Digital data collection minimizes the risk of errors associated with manual data entry. Validation rules can be implemented to ensure data accuracy at the point of entry.
- Real-Time Data Availability: Digital data collection provides real-time access to collected data, enabling teams to make informed decisions promptly. This is particularly valuable for time-sensitive projects.
- Enhanced Data Security: Digital data collection tools often come with built-in security features, protecting sensitive information from loss or unauthorized access.

- Time Efficiency: Streamlining data collection processes reduces the time required for manual entry, verification, and reconciliation. Teams can focus on more value-added tasks.
- Cost Savings: By eliminating the need for paper, printing, and manual data entry, digital data collection methods contribute to cost savings over time.
- Improved Data Analysis: Digital data is easier to analyze and interpret. Teams can leverage data visualization tools and analytics to gain valuable insights for decision-making.
- Reduced Environmental Impact: Shifting to digital data collection aligns with sustainability goals by reducing paper consumption and the environmental impact associated with traditional data collection methods.
- Increased Collaboration: Digital data collection tools facilitate collaboration among team members by providing a centralized platform for data sharing and updates.
- Scalability: Digital solutions can easily scale to accommodate growing data collection needs without the logistical challenges associated with traditional methods.
- Adaptability to Changing Conditions: Digital data collection methods allow teams to adapt quickly to changing conditions or requirements, ensuring flexibility in data collection processes.

The following apps are designed to perform well in adverse weather conditions:

- **Fulcrum**: Fulcrum is known for its offline capabilities, allowing data collection even in areas with poor or no connectivity. This makes it suitable for adverse weather conditions where network reliability might be an issue.
- **GeoODK Collect**: An open-source app based on Open Data Kit, GeoODK Collect is designed for offline data collection. It is suitable for adverse weather conditions and can store data locally on the device until a connection is available for synchronization.
- **ArcGIS Survey123**: Survey123 is part of the ArcGIS suite and is designed to work in challenging field conditions. It supports offline data collection and has features to ensure data integrity and reliability in adverse weather.
- **KoBoToolbox**: KoBoToolbox is designed to work in various field conditions, making it suitable for adverse weather. It allows for offline data collection and provides flexibility in designing forms for different types of surveys.
- **CommCare**: CommCare is designed for frontline workers and can handle offline data collection effectively. It is used in various challenging environments, including adverse weather conditions.
- **Magpi**: Magpi supports offline data collection, making it suitable for adverse weather conditions where network connectivity may be inconsistent. It also provides real-time monitoring of data collection activities.

- **Formotus**: Formotus is a mobile forms platform that supports offline data collection. It offers flexibility in creating custom forms and can be used in adverse weather conditions where connectivity might be a concern.

7.3.2 Standardize Data Formats

Current State	Different file formats hinder interoperability and create compatibility issues.
Recommendation	Standardizing data formats while acknowledging the use of Excel for analysis is crucial for promoting consistency, interoperability, and effective data analysis within PGST. The easiest way to achieve this is by incorporating the data conversion tools.
Example	Establish guidelines for data storage in CSV or Excel formats for consistency. This ensures compatibility across different departments while maintaining the convenience of using Excel for data analysis.

How to achieve standardization in Data Formats?

- Define Common Data Formats: Clearly define the common data formats that should be used across all teams and departments. This includes specifying file types, data structures, and encoding standards.

- Consider Industry Standards: Align data formats with industry standards whenever applicable. This ensures compatibility with external partners, reduces data conversion efforts, and facilitates seamless data exchange.

- Document Data Format Guidelines: Document guidelines on data formats in a centralized document that is accessible to all teams. Include information on how to structure data files, naming conventions, and any relevant metadata requirements.

- Provide Conversion Tools: Offer tools or guidelines for converting data to different formats when necessary. This is particularly important when collaborating with external entities that may use different standards.

7.4 Data Storage and Archival

7.4.1 Implement Data Retention Policies

Current State	Lack of data retention policies leads to unnecessary storage space consumption.
Recommendation	Developing and implementing data retention policies is crucial for managing server space effectively, ensuring that only relevant and necessary data is retained.
Example	Define timeframes for storing active data on servers. For instance, keep the last five years of data on the server and archive older data. Establish archival processes for older data. This ensures optimal server space utilization.

How to create and implement data retention policies?

- Identify Data Categories: Categorize data based on its importance, sensitivity, and regulatory requirements. Classify data into categories, such as critical, important, and non-essential.
- Understand Legal and Regulatory Requirements: Research to understand legal and regulatory requirements applicable to data retention in your industry and region. Ensure that data retention policies align with compliance standards.
- Define Retention Periods: Specify the retention periods for each data category. Clearly define how long different types of data should be retained based on business needs, legal obligations, and historical significance.
- Include Archival and Deletion Processes: Outline processes for archiving data that needs to be retained for historical or compliance reasons. Similarly, establish procedures for the secure and permanent deletion of data that has reached the end of its retention period.
- Define Ownership and Responsibility: Clearly define the ownership and responsibility for data retention within PGST. Designate individuals or teams responsible for implementing and enforcing data retention policies.
- Document Policies: Document the data retention policies in a centralized document or policy handbook. Ensure that this document is easily accessible to all relevant personnel.

Implement Data Retention Policies:

- Communicate Policies: Communicate the data retention policies to all employees within the Natural Resources Department. Ensure that everyone is aware of the guidelines and understands their role in compliance.
- Automate Retention Processes: Implement automated tools and processes to enforce data retention policies. Automation reduces the risk of human error and ensures consistent application of policies.

- Integrate with Data Management Systems: Integrate data retention policies with existing data management systems and servers. Ensure that the policies are seamlessly enforced within the day-to-day operations of PGST.

- Periodic Policy Reviews: Periodically review and update data retention policies to ensure they remain aligned with changes in business needs, regulations, and technology. Solicit feedback from stakeholders to improve the effectiveness of policies.

- Document Deletion Processes: Document processes for the secure deletion of data. Ensure that when data reaches the end of its retention period, it is deleted in a manner that complies with data protection and privacy standards.

- Backup and Disaster Recovery Considerations: Integrate data retention policies with backup and disaster recovery plans. Ensure that retained data is included in backup routines and can be restored if needed.

- Legal Hold Procedures: Establish procedures for legal holds in case of litigation or investigations. Ensure that data relevant to legal proceedings is preserved as required by law.

7.4.2 Leverage Cloud Storage for Images

Current State	Image data stored in private iClouds poses risks and lacks central management.
Recommendation	Utilize cloud storage services for centralized and secure image data storage. Utilizing cloud storage services for centralized and secure image data storage offers several advantages, including scalability, accessibility, and robust security features.
Example	Integrate Microsoft OneDrive for image storage. This allows teams to securely store and access image data on a centralized location, reducing the risk of data loss.

How to effectively leverage cloud storage services for centralized and secure image data storage?

- Choose a Cloud Storage Provider
    - Evaluate Options: Assess different cloud storage providers such as Amazon S3, Google Cloud Storage, Microsoft Azure Blob Storage, or specialized image storage services like Amazon S3 Glacier Deep Archive for long-term archival.
    - Consider Security Features: Choose a provider with robust security features, including encryption at rest and in transit, access controls, and compliance certifications (e.g., ISO 27001, SOC 2).
    - Scalability and Performance: Consider the scalability and performance of the cloud storage service, ensuring it can handle the volume of image data and provide low-latency access.

- Plan Your Cloud Storage Architecture
  - Organize Storage Structure: Design a logical and organized structure for storing image data. Consider organizing data based on projects, departments, or any other relevant categorization.
  - Use Containers or Buckets: Leverage containers or buckets provided by the cloud storage service to compartmentalize and organize image data. This helps in maintaining a structured hierarchy.
  - Implement Versioning: Enable versioning for your cloud storage buckets to track changes to image files over time. This ensures that previous versions of images can be restored if needed.
  - Utilize Metadata: Leverage metadata to add descriptive information to image files. This can include details such as creation date, project name, or any other relevant information for easy retrieval.
- Ensure Security and Access Controls
  - Encryption: Enable encryption for data at rest and in transit. Most cloud storage providers offer mechanisms to encrypt data, providing an additional layer of security.
  - Access Controls: Implement fine-grained access controls to restrict who can access, modify, or delete image data. Assign permissions based on roles and responsibilities within the organization.
  - Multi-Factor Authentication (MFA): Enable multi-factor authentication for accessing the cloud storage account. This adds an extra layer of security, especially for accounts with administrative privileges.
  - Audit Logging: Turn on audit logging features provided by the cloud storage service. Regularly review logs to monitor access patterns and detect any suspicious activity.
- Backup and Disaster Recovery
  - Regular Backups: Establish a regular backup schedule to create redundant copies of image data. This ensures data resilience and minimizes the risk of data loss.
  - Disaster Recovery Plan: Develop a comprehensive disaster recovery plan that includes procedures for recovering image data in case of unexpected events. Test the plan periodically to ensure its effectiveness.

- Cost Optimization
  - Data Lifecycle Management: Implement data lifecycle management policies to automatically transition less frequently accessed images to lower-cost storage tiers or archives.
  - Monitor and Optimize Storage Costs: Regularly monitor storage usage and costs. Optimize storage configurations based on usage patterns to ensure cost-effectiveness.

7.4.3 Reduce Reliance on External Drives

Current State	Teams storing data on external drives risk data loss and security breaches.
Recommendation	Discourage the use of external drives and promote centralized storage solutions. Discouraging the use of external drives and promoting centralized storage solutions offers several advantages for organizations in terms of security, collaboration, and data management.
Example	Migrate data from external drives to the centralized SharePoint repository. This ensures data consistency, centralizes access, and mitigates the risk of data loss from individual external drives.

Key reasons to discourage the use of external drives and promote centralized storage solutions are as follows:

- Security and Access Control:
  - External Drives: External drives, such as USB flash drives or external hard disks, can be easily lost or stolen. This poses a significant security risk as sensitive data may be accessed by unauthorized individuals.
  - Centralized Storage: Centralized storage solutions often come with robust security features, including access controls, encryption, and authentication mechanisms. This helps protect sensitive data and ensures that access is restricted to authorized users.
- Data Redundancy and Version Control:
  - External Drives: Managing data across multiple external drives can lead to redundancy and version control issues. It becomes challenging to track and maintain the latest versions of files, leading to potential inconsistencies.
  - Centralized Storage: Centralized storage solutions provide version control mechanisms, ensuring that users are working with the latest versions of files. This reduces the risk of using outdated or incorrect data and promotes collaboration.

- Collaboration and Remote Access:
    - External Drives: External drives are typically limited to local access, making collaboration challenging, especially for teams working in different locations. Remote access may not be feasible without physically transferring the drive.
    - Centralized Storage: Centralized storage solutions are accessible from anywhere with an internet connection, facilitating collaboration among team members, including those working remotely. This enhances productivity and teamwork.
- Data Backup and Recovery:
    - External Drives: External drives are susceptible to hardware failures. Data loss can occur if the drive malfunctions or becomes damaged. Regular backups are often manual and may be neglected.
    - Centralized Storage: Centralized storage solutions often include automated backup features, reducing the risk of data loss. Regular backups and recovery processes can be established to ensure data integrity and availability.
- Scalability and Flexibility:
    - External Drives: Managing data across multiple external drives can be cumbersome and lacks scalability. As data grows, the need for additional external drives may lead to inefficiencies.
    - Centralized Storage: Centralized storage solutions are designed to scale with PGST's data needs. They offer flexibility to adapt to changing storage requirements without the logistical challenges associated with external drives.
- Compliance and Governance:
    - External Drives: Ensuring compliance with industry regulations or internal governance policies can be challenging when data is dispersed across external drives with varying levels of security and control.
    - Centralized Storage: Centralized storage solutions enable PGST to implement and enforce compliance and governance policies consistently. This is crucial for industries with strict regulatory requirements.
- Cost-Efficiency:
    - External Drives: Managing multiple external drives may lead to hidden costs, including the need for additional drives, potential data loss incidents, and time-consuming manual processes.

  - Centralized Storage: Centralized storage solutions provide a cost-efficient and centralized approach to data management. They often offer predictable pricing models and reduce the total cost of ownership.

7.5 Data Security and Compliance

7.5.1 Enhance Data Security Measures

Current State	Open access to folders poses significant security threats.
Recommendation	Implementing robust data security measures, including folder-level access controls, is critical to safeguarding sensitive information and ensuring that data is accessed only by authorized individuals.
Example	Restrict access to sensitive folders by assigning specific permissions. For instance, only authorized personnel should have access to folders containing sensitive data, ensuring data security.

How to implement security measures?

- Conduct Data Security Assessment:
  - Identify Sensitive Data: Conduct a thorough assessment to identify sensitive and confidential data within PGST.
  - Assess Security Risks: Evaluate potential security risks and vulnerabilities associated with the identified data. Consider factors, such as data storage, transmission, and access points.
- Define Access Control Policies:
  - Categorize User Roles: Categorize users into roles based on their responsibilities and access requirements.
  - Define Access Levels: Specify access levels for each user role, including read-only, write, edit, and delete permissions.
  - Apply the Principle of Least Privilege: Follow the principle of least privilege, granting users the minimum level of access needed to perform their job responsibilities.
- Implement Folder-Level Access Controls:
  - Folder Structure Design: Design a logical folder structure that aligns with PGST's workflow. Group files and folders based on projects, departments, or access requirements.
  - Apply Access Controls: Implement folder-level access controls to restrict access to specific users or groups. Most file storage systems and platforms (such as SharePoint or Google Drive) provide granular control over folder permissions.

  - Regularly Review and Update Access: Conduct regular reviews of folder-level access controls to ensure they align with the current organizational structure and personnel changes.
- Use Encryption:
  - Implement Encryption at Rest: Enable encryption at rest to secure data stored on servers or in the cloud. This ensures that even if unauthorized access occurs, the data remains unreadable without the appropriate decryption keys.
  - Enable Encryption in Transit: Encrypt data during transmission to prevent eavesdropping and unauthorized interception. Use secure protocols such as HTTPS for web-based file transfers.
- Authentication Mechanisms:
  - Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security. This requires users to provide multiple forms of identification before gaining access.
  - Strong Password Policies: Enforce strong password policies, including requirements for complexity, length, and regular password updates.
- Auditing and Monitoring:
  - Enable Audit Logging: Turn on audit logging features to track user activities, including file access, modifications, and permission changes.
  - Regularly Review Logs: Regularly review audit logs to detect and investigate any suspicious activities or unauthorized access.
- Data Loss Prevention (DLP):
  - Implement DLP Solutions: Deploy DLP solutions to monitor and control the movement of sensitive data within and outside PGST.
  - Automated Alerts for Policy Violations: Set up automated alerts for potential policy violations, ensuring that security incidents are detected and addressed promptly.
- Regular Security Training:
  - Security Awareness Training: Conduct regular security awareness training for employees. Educate them on the importance of data security, recognizing phishing attempts, and adhering to security best practices.

- Incident Response Plan:
  - Develop an Incident Response Plan: Develop a comprehensive incident response plan to outline steps to be taken in the event of a security breach. Ensure that the plan is regularly tested and updated.
  - Communication Protocols: Establish communication protocols for notifying relevant parties, including IT, management, and affected users, in the event of a security incident.
- Regular Security Audits:
  - Periodic Security Audits: Conduct regular security audits to assess the effectiveness of implemented security measures. Identify areas for improvement and address vulnerabilities promptly.
  - External Penetration Testing: Consider external penetration testing to simulate real-world attacks and identify potential weaknesses in the security infrastructure.

7.5.2 Develop Standard Operating Procedures (SOPs) and Frequently Asked Questions (FAQs)

Current State	Lack of SOPs and FAQs contributes to data management challenges.
Recommendation	Developing SOPs and FAQs are essential to ensure consistent practices and facilitate knowledge transfer within an organization.
Example	Create training modules on data management, access controls, and best practices. Provide ongoing training sessions to ensure all team members are familiar with standardized procedures.

How to create Standard Operating Procedures (SOPs)?

- Introduction: Clearly define the purpose of the SOPs and their importance in maintaining consistent practices.
- Scope: Outline the specific processes and activities covered by the SOPs.
- Roles and Responsibilities: Clearly define the roles and responsibilities of individuals involved in the processes outlined in the SOPs.
- Procedure Details: Break down each procedure into detailed steps. Use a clear and concise language to ensure understanding.
- Flowcharts or Diagrams: Supplement text with flowcharts or diagrams to visually represent the procedures and enhance comprehension.
- Key Performance Indicators (KPIs): Define relevant KPIs to measure the effectiveness of the processes outlined in the SOPs.

- Document Control: Establish a system for version control, ensuring that SOPs are regularly reviewed and updated as needed.
- Compliance and Quality Standards: Specify any compliance requirements or quality standards that must be adhered to during the execution of the procedures.
- Training Requirements: Identify specific training requirements for individuals involved in the processes covered by the SOPs.
- Approval and Sign-off: Include a section for approval and sign-off by relevant stakeholders to formalize the acceptance of the SOPs.

7.6 Data Quality and Accuracy

7.6.1 Establish Data Quality Assurance Procedures

Current State	Data accuracy relies on trust without formalized procedures.
Recommendation	Developing data quality assurance procedures is essential to validate and ensure accuracy of data within PGST.
Example	Implement periodic data audits where a designated team reviews a sample of collected data to identify and rectify inaccuracies. This ensures ongoing data accuracy.

How to establish data quality assurance?

- Define Data Quality Objectives:
  - Identification Identify Key Data Elements: Identify and prioritize the key data elements critical to PGST's operations and decision-making.
  - Establish Data Quality Metrics: Define specific metrics and criteria for assessing data quality, such as accuracy, completeness, consistency, and timeliness.
  - Set Quality Thresholds: Establish acceptable thresholds for each data quality metric. These thresholds serve as benchmarks for determining data quality levels.
- Data Profiling:
  - Utilize Data Profiling Tools: Utilize data profiling tools to analyze and understand the characteristics of the data, including patterns, distributions, and anomalies.
  - Identify Data Anomalies: Identify and document any anomalies, outliers, or discrepancies within the data during the profiling process.
  - Document Data Source Information: Document information about data sources, including data origins, collection methods, and any transformations applied.

- Data Validation and Cleansing:
    - Implement Validation Rules: Define and implement validation rules to check data against predefined criteria. This ensures that data adheres to specified standards and business rules.
    - Develop Cleansing Procedures: Develop procedures for data cleansing to address inaccuracies, inconsistencies, or missing values. This may involve correcting, enriching, or removing problematic data.
    - Integrate Automated Validation: Integrate automated validation processes into data pipelines to perform real-time checks during data ingestion.
- Data Standardization:
    - Standardize Data Formats: Define and implement standards for data formats, units of measurement, and naming conventions to ensure consistency across datasets.
    - Address Data Discrepancies: Develop procedures to address discrepancies when integrating data from different sources. This may involve mapping and transforming data to a standardized format.
- Implement Data Quality Monitoring:
    - Real-Time Monitoring: Establish real-time monitoring mechanisms to continuously assess data quality. This involves setting up alerts for deviations from established thresholds.
    - Scheduled Quality Checks: Conduct scheduled data quality checks at regular intervals to ensure ongoing monitoring and early detection of issues.
    - Logging and Reporting: Implement logging mechanisms and generate regular reports on data quality metrics. These reports can be used to track trends and identify areas for improvement.
- Data Quality Governance:
    - Define Data Quality Roles and Responsibilities: Clearly define roles and responsibilities for individuals involved in data quality governance. This includes data stewards, data owners, and other relevant stakeholders.
    - Establish Data Quality Policies: Develop and document data quality policies that outline the organization's commitment to maintain high-quality data.
    - Conduct Data Quality Training: Provide training to personnel involved in data management to ensure they understand the importance of data quality and their roles in maintaining it.

- Feedback Mechanism:
  - Establish User Feedback Channels: Establish channels for users to provide feedback on data quality issues they encounter. This can include data entry errors, discrepancies, or any other anomalies.
  - Develop Incident Resolution Process: Develop a clear process for addressing reported data quality issues, including investigation, resolution, and communication with stakeholders.
- Documentation and Metadata Management:
  - Maintain Metadata Documentation: Document metadata information associated with datasets, including data lineage, definitions, and usage guidelines.
  - Implement Version Control for Data Quality Rules: Implement version control for data quality rules to track changes and updates over time.
  - Maintain Data Quality Documentation: Regularly review and update documentation related to data quality procedures and practices to ensure accuracy and relevance.
- Continuous Improvement:
  - Conduct Regular Data Quality Audits: Conduct regular data quality audits to assess the effectiveness of data quality procedures and identify areas for improvement.
  - Establish Feedback Loop for Improvement: Establish a feedback loop for continuous improvement based on the results of data quality audits and user feedback.
  - Adapt to Changing Requirements: Stay adaptable to changing business requirements and technology advancements, adjusting data quality procedures accordingly.

7.6.2 Implement Investigation Procedures for Inaccuracies

Current State	Lack of investigation procedures for inaccurate data.
Recommendation	Establishing investigation procedures is crucial for identifying and rectifying inaccuracies in data.
Example	Assign a data quality team to investigate and correct inaccuracies promptly. Develop a systematic process form reporting and resolving data discrepancies.

How to set up effective investigation procedures?

- Define Triggers for Investigation:
  - Thresholds Set Thresholds and Tolerances: Set predefined thresholds or tolerances for key data quality metrics (e.g., accuracy, completeness). When data falls outside these thresholds, it triggers an investigation.

  - Gather User Feedback: Establish a system for users to report data inaccuracies or anomalies they encounter during their work.
  - Implement Automated Alerts: Implement automated alerts and notifications to immediately flag potential inaccuracies or deviations from established norms.
- Create an Investigation Team:
  - Define Roles and Responsibilities: Clearly define roles and responsibilities for the investigation team, including data stewards, analysts, and subject matter experts.
  - Cross-Functional Collaboration: Ensure a cross-functional collaboration involving members from relevant departments to bring diverse perspectives to the investigation process.
  - Involve Data Owner: Involve data owners who are responsible for specific datasets in the investigation process.
- Initiate the Investigation:
  - Document the Issue: When an inaccuracy is identified, document the issue comprehensively, including a description of the problem, affected data, and potential impact.
  - Assess the Priority: Assess the priority of the investigation based on the significance of the data inaccuracy and its potential impact on business operations.
  - Assign Investigation Leads: Assign leads for the investigation who will be responsible for coordinating efforts, communicating findings, and ensuring timely resolution.
- Data Profiling and Analysis:
  - Utilize Data Profiling Tools: Utilize data profiling tools to conduct a detailed analysis of the affected data. Identify patterns, anomalies, and potential causes of inaccuracies.
  - Perform Root Cause Analysis: Perform root cause analysis to understand the underlying reasons for data inaccuracies. This may involve examining data sources, transformation processes, or manual data entry procedures.
  - Compare with Source Systems: Compare the inaccurate data with the original source systems to identify any discrepancies introduced during data integration or transformation.
- Documentation and Reporting:
  - Create Investigation Reports: Develop comprehensive investigation reports that include findings, root causes, and recommended corrective actions.

  - Document Changes Made: Document any changes made to rectify inaccuracies. This documentation is essential for transparency and audit purposes.
  - Communicate Findings: Communicate investigation findings to relevant stakeholders, including data owners, management, and end-users. Provide clear explanations and timelines for resolution.
- Corrective Actions:
  - Implement Immediate Corrections: Implement immediate corrective actions for critical inaccuracies to prevent further impact on business processes.
  - Develop Long-Term Solutions: Develop long-term solutions to address underlying issues and prevent similar inaccuracies in the future. This may involve process improvements, system enhancements, or additional training.
  - Validate Corrections: Validate that corrective actions effectively rectify the inaccuracies. Perform validation checks and confirm that data quality metrics are within acceptable thresholds.
- Continuous Improvement:
  - Conduct Review and Feedback Loop: Conduct regular reviews of the investigation procedures to identify areas for improvement. Establish a feedback loop with the investigation team to capture lessons learned.
  - Adapt Procedures: Adapt investigation procedures based on the evolving nature of data, changes in business processes, or feedback from stakeholders.
  - Training and Awareness: Provide training to personnel involved in data management on lessons learned from investigations. Enhance awareness to prevent similar inaccuracies in the future.
- Documentation Management:
  - Implement Version Control: Implement version control for investigation reports and related documentation. This ensures a historical record of inaccuracies, investigations, and resolutions.
  - Maintain Centralized Repository: Maintain a centralized repository for all investigation documentation, making it easily accessible for future reference and audits.

7.7 Data Sharing and Collaboration

7.7.1 Enhance Data Sharing Mechanisms

Current State	Email and OneDrive usage lead to version control challenges and redundancy.
Recommendation	Implement a centralized collaboration platform for seamless data sharing. Implementing a centralized collaboration platform is crucial for seamless data sharing within PGST. A well-designed platform fosters collaboration, enhances communication, and ensures that data is shared securely and efficiently.
Example	Utilize Microsoft Teams for internal communication and file sharing. This platform ensures version control, permissions management, and centralized space for collaboration.

How to implement a centralized collaboration platform?

- Define Objectives and Requirements:
  - Identify Collaboration Goals: Clearly define the objectives of the collaboration platform, such as improving communication, sharing project updates, and facilitating data exchange.
  - Assess User Requirements: Gather requirements from end-users to understand their needs and preferences for collaboration tools and features.
- Select a Collaboration Platform:
  - Consideration of Platforms: Evaluate different collaboration platforms, such as Microsoft Teams, Slack, SharePoint, or other industry-specific platforms based on PGST's needs.
  - Integration Capabilities: Consider the integration capabilities of the platform with existing systems, data sources, and tools used within PGST.
  - Security and Compliance: Ensure that the selected platform adheres to security standards and compliance requirements relevant to PGST.
- Customization and Configuration:
  - Adapt to Organizational Structure: Customize the platform to align with the PGST’s structure, creating teams, channels, or workspaces that mirror departmental or project-based divisions.
  - Configure Access Controls: Set up access controls and permissions to ensure that users have appropriate levels of access based on their roles and responsibilities.
  - Customize Branding and User Interface: Customize the platform's branding and user interface to reflect PGST's identity and enhance user experience.

- Integrate with Existing Tools:
  - Connectivity with Productivity Tools: Integrate the collaboration platform with existing productivity tools, such as Microsoft 365, Google Workspace, or project management tools, to streamline workflows.
  - Data Integration: Implement data integrations to enable seamless sharing of data and documents directly within the collaboration platform.
- Training and Onboarding:
  - Training Programs: Develop training programs to familiarize users with the features and functionalities of the collaboration platform. This may include live training sessions, documentation, or video tutorials.
  - Onboarding Process: Establish an onboarding process for new employees to ensure they are introduced to the collaboration platform as part of their orientation.
- Encourage User Adoption:
  - Communication and Promotion: Communicate the benefits of the collaboration platform to users and promote its use through internal communications, newsletters, and team meetings.
  - Feedback Mechanism: Establish a feedback mechanism to gather input from users and continuously improve the platform based on their needs.
- Security Measures:
  - Encryption and Data Security: Implement encryption and other security measures to protect sensitive data shared on the platform.
  - Access Controls: Enforce strict access controls to ensure that only authorized users can access and contribute to specific channels or projects.
  - Regular Security Audits: Conduct regular security audits to identify and address any vulnerabilities in the collaboration platform.
- Monitoring and Analytics:
  - Usage Analytics: Implement tools for monitoring platform usage and analytics to gain insights into how teams are utilizing the collaboration features.
  - Performance Monitoring: Monitor the performance of the collaboration platform to identify and address any issues promptly.

- Scale and Adapt:
    - Scalability: Ensure that the collaboration platform is scalable to accommodate the growing needs of PGST, including an increasing number of users and data volumes.
    - Adaptability to Changes: Stay adaptable to changes in organizational structure, business processes, and technology advancements. Update the collaboration platform accordingly.
- Feedback and Continuous Improvement:
    - User Surveys: Conduct user surveys periodically to gather feedback on the collaboration platform's effectiveness and identify areas for improvement.
    - Iterative Updates: Implement iterative updates and enhancements based on user feedback and changing organizational requirements.

7.7.2 Implement Version Control Mechanisms

Current State	Lack of version control leads to data duplications and challenges in maintaining the latest version.
Recommendation	Implement version control mechanisms to track changes and avoid redundancy.
Example	Utilize version control features within Microsoft SharePoint or implement third-party versioning tools. This allows teams to track changes, access previous versions, and avoid data duplications.

How to implement version control mechanism?

- Choose a Document Versioning System
    - Select a Versioning Tool: Choose a document versioning tool or system. This could be a version control system (e.g., SharePoint, Google Drive, or other cloud-based collaboration tools).
- Set Up a Document Repository
    - Create a Document Repository: Set up a centralized repository where documents will be stored. Ensure it supports versioning features.
    - Organize Folders and Categories: Organize the repository with clear folder structures and categories to facilitate easy navigation.

- Document Versioning Policies
  - Define Versioning Policies: Establish clear versioning policies, such as when a new version should be created (e.g., after significant edits, approvals, or at specific project milestones).
  - Semantic Versioning: Consider adopting semantic versioning for documents, indicating major, minor, and patch changes.
- Access Controls and Permissions
  - Access Controls: Set access controls to restrict document editing and versioning permissions based on roles and responsibilities.
  - User Permissions: Define user permissions, ensuring that only authorized individuals can make changes or approve new versions.
- Document Check-Out and Check-In
  - Check-Out Mechanism: Implement a check-out mechanism where users need to "check out" a document before making edits. This prevents conflicting changes.
  - Check-In Process: Define a clear process for checking in documents, ensuring that changes are properly documented and versioned.
- Document Collaboration and Review
  - Collaboration Features: Use collaboration features within the chosen document management system to enable real-time collaboration and comments.
  - Review Processes: Establish review processes to ensure that major changes or new versions undergo proper scrutiny before finalization.
- Automatic Versioning and Timestamps
  - Automatic Versioning: Enable automatic versioning within your document management system so that new versions are created automatically when changes are saved.
  - Timestamps: Ensure that each version is timestamped, providing a clear record of when changes were made.

8 Conclusion

In conclusion, the Data Management Analysis & Recommendation Report for the Port Gamble S'Klallam Tribe's (PGST) Natural Resources Department has identified key challenges in the current data management practices. These include a lack of centralized data repository, non-standard naming conventions, reliance on paper forms for data collection, and several other issues related to data security, access control, and accuracy investigation procedures.

To address these challenges, a comprehensive set of recommendations has been proposed. These include establishing a centralized data repository, implementing access control policies, standardizing file naming conventions, promoting digital data collection, implementing data retention policies, leveraging cloud storage for images, reducing reliance on external drives, enhancing data security measures, implementing version control mechanisms, implementing investigation procedures for inaccuracies, and enhancing data sharing mechanisms. Each recommendation is accompanied by an example for better understanding and implementation.

The proposed plan aims to establish best practices and consistency in data management, improve document control, and enhance the utilization of Microsoft 365, OneDrive, Outlook, and Natural Resources Server. It also guides the organization in effective file naming conventions, version control, keyword usage, metadata implementation, document control processes, and archival, as well as seamless integration with geospatial and mapping best practices.

By implementing these recommendations, PGST's Natural Resources Department can expect to see significant improvements in their data management practices, leading to more efficient and effective operations. The benefits of some of these recommendations have been explained in detail in the report.

The success of this plan will depend on the commitment and active participation of all members of the PGST's Natural Resources Department. It is hoped that this report will serve as a valuable guide in their journey towards improved data management.

9 Contact Information

Himanshu Saluja

Business Analyst

Digital Technology & Innovation, Technology Office

Stantec

This report has been reviewed and approved by:

Ross Poulin

Principal | Project Information Management Systems Leader

Digital Technology & Innovation | Technology Office

Stantec

PGST Representative's Name: **Roma Call**

PGST Representative's Title: Director, Natural Resources Department, Port Gamble S’Klallam Tribe