



Minimum Implementation Standards for Network Projects

Version: 1.1

Date Released: 10/6/2016

Last Updated: 11 October 2016

Table of Contents

1	Introduction.....	2
2	Database Standards.....	2
3	Water Quality.....	3
4	Protected Records.....	3

Revision History Log:

Previous Version #	Revision Date	Author(s)	Changes Made	Reason for Change	New Version #
NA	8/17/2016	Frakes, Kingston	First version	NA	1.0
1.0		Frakes, Kingston	1. Clarified that minimum standards apply to new databases as well as existing 2. Added protected status guidance	1. Central office does not currently have the resources to implement all standards at present 2. Integration of QAP guidance	1.1

1 Introduction

This document describes the minimum level of policy implementation by the central office for any network assistance project implemented by the central office. Minimum implementation does not imply never going beyond the minimum; however, in cases where time/resources are a constraint, these standards will ensure that projects are manageable.

These standards apply to all network projects, including those developing a new database application as well as working with existing systems.

The target audience for these standards is central office staff.

Although we hope to always at least follow the minimum, we anticipate cases where even doing the “minimum” is unattainable/unreasonable given the existing resources. Thus, exceptions will be accommodated on a case-by-case basis with the expectation that they be negotiated and documented in the project plan.

These minimum implementation standards will be updated regularly as policy is introduced/revised and as the central office determines reasonable levels of minimal implementation.

2 Database Standards

See <https://irma.nps.gov/DataStore/Reference/Profile/2224205?Inv=true> for explanation of standards

For any project involving an existing database that needs revision/improvement, the central office will ensure that the database meets the following standards:

General Database

- Referential Integrity (1.2)
- Data Stand Alone (1.4)

Table Organization and Naming

- Table Description (2.2)
- Primary Keys (2.4)
- Unique Records (2.8)
- Distinct Lookup Tables (2.9)

Column Organization and Naming

- Column Names Representing Unit of Measure (3.6)
- Column Descriptions (3.7)
- Geospatial Units and Datum (3.9)
- Default Values (3.12)
- Zero-Length Strings (3.13)

3 Water Quality

For all network assistance projects involving discrete water quality data, the central office will ensure that there is the capacity to provide the data to the Water Resource Division (WRD) instance of EQuIS.

These databases that are developed/augmented by the central office will have an EQuIS EDD export routine for submission to WRD. Specific guidance on the mapping is found in the “Water Resource Division EQuIS EDD Mapping: IMD Implementation” [document](#). At a minimum, the central office will:

- Map data to all required fields defined by EQuIS
- Attempt to map all data collected by the network that is considered optional by the WRD.

In cases where there is water quality data that does not clearly have an appropriate location in the EQuIS EDD, the central office will not attempt to determine work-arounds or negotiate with the WRD about additions/enhancements to the existing EDD.

Finally, the central office will direct networks to request that labs submit data to Networks in WQX structure. If labs are unaware of EQuIS WQX, a template is [here](#).

4 Protected Records

Because data are intended to be open and public by default, Networks will identify potential types of data that must be classified as protected (See [QAP Guidance](#)) as early as possible in the data management workflow so as to limit the risk of accidental dissemination (ideally immediately upon data entry). Networks will work with appropriate park staff (typically resource management chiefs or above) to define what data are protected, the degree of protection warranted, and if/how data will be disseminated.

Types of information to evaluate include:

- [Resource Data and Information](#) – Information about biological taxa
- [Location Data and Information](#) – Location-specific information
- [Personally Identifiable Information](#) – Information that is used to uniquely define an individual

One of three levels of protected status are to be assigned to each of the main information types to generate a protected status matrix (See Example Table 4.1):

- [Legally Protected](#). Covered under existing statute as being exempt from public dissemination

- Operationally Protected: Data withheld from release to protect resources or site fidelity but may be subject to release upon request.
- Not Protected: Data is neither legally nor operationally sensitive and therefore has does not have any distribution restrictions conditional on protected status

Example Table 4.1. Example table summarizing data protection standards for inclusion with quality assurance plans developed for protocols implemented by the NPS Inventory & Monitoring Division. With the exceptions noted, all data collected are to be made publicly available in a timely fashion.

Type of Data		Level of Protection	Rules for Dissemination
Resource Data and Information			
	T&E Species Locations	Legally Protected	Locations of observations reported at park centroid only.
	<i>Galax</i> species locations	Legally Protected	Commercially valuable; location information redacted from all dissemination
	T&E migratory shorebird locations	Legally Protected	Locations of observations reported at park centroid for three years; fuzzed to within 50m thereafter.
Location Data and Information			
	Cave entrances	Legally protected	Redacted
	Spring locations	Legally protected	Redacted; features associated with protected archaeological sites.
	Permanent Sampling Locations	Operationally protected	Coordinates provided upon request only. Relative position shown in reports
Personally Identifiable Information			
	Non-NPS Staff Information	Legally Protected	All but first name and last initial redacted from public release

Managing Resource Data and Information

- The master taxonomy lookup table will contain the current protected status for each species tracked by the protocol. This status should be updated regularly. It may also contain a Protected Status Notes column (entry optional) that can be used to describe the reason for the protected status, when it was updated, etc.
- When a taxon is recorded in an observation table, it will inherit the current protected status from the master taxonomy lookup table, with the ability of defined user roles to change the protected status of a specific taxon observation between initial data entry and certification
- Reporting of a taxon (whether by export, report, query, etc.) should use the protected status defined in the taxon observation table (not the lookup table) along with the dissemination rules to determine the content of the output

Managing Location Data and Information

- The site/location table will have a required protected status column and an optional Protected Status Notes column
- Reporting of any location (whether by export, report, query, etc.) should use the protected status defined at the site/location table along with the dissemination rules to determine the content of the output

Managing Personally Identifiable Information (PII)

- The staff/contact table will have a required protected status column and an optional Protected Status Notes column
- Reporting of any staff/person (whether by export, report, query, etc.) should use the protected status defined at the staff/person table along with the dissemination rules to determine the content of the output

Inventory and Monitoring Division

Protected Status Lookup Table

The following ProtectedStatus lookup table will be used

Code	Name	Description
LP	Legally Protected	Covered under existing statute as being exempt from public dissemination
OP	Operationally Protected	Data withheld from release to protect resources or site fidelity but may be subject to release upon request.
NP	Not Protected	Data is neither legally nor operationally sensitive and therefore has does not have any distribution restrictions conditional on protection status