**HydroServer Data Access Control Requirements**

1. ***HydroServer administrators and data owners should be able to control access to data resources hosted on a HydroServer*** – this is the base requirement and the one that drives all of the following requirements.
2. ***Access to at least 4 classes of data will be supported*** – data will be classified based on how it can be accessed. For read access, the following four classes of data will be supported:
   1. ***Type 1 Public Data No Restrictions*** – Both metadata and data are public. Tracking or identification of users is not required for read access. Unauthenticated users can read.
   2. ***Type 2 Tracked Public Data*** – Metadata are public, and the data can be read by anyone that has supplied an identity.
   3. ***Type 3 Public Metadata, Restricted Data*** – Metadata are public, but only those who have identified themselves and have been authorized can read the data.
   4. ***Type 4 Restricted Data*** – Both metadata and data are private and can only be read by those who have identified themselves and have been authorized.
3. ***HydroServer access control will support create, read, update, and delete operations on data resources*** – the access control system will facilitate new functionality that enables create, read, update, and delete access for data resources through web service interfaces , whereas currently only read access is possible. The requirements in this document are only for the access control system that would enable create, update, and delete operations through web services and do not specify the functionality of the services that would be required.
4. ***Exceptions in firewalls to allow outgoing communication of data and incoming requests should be minimized*** – to avoid problems with firewalls and to enable HydroServer to be more interoperable with other systems, HydroServer web services (e.g., data access, authentication, authorization) will work over standard ports that are not likely to be blocked by University network administrators.
5. ***Requests from unauthenticated data consumers*** – requests from unauthenticated data consumers will be supported by the system, but will be limited to reading public metadata and data for which access control restrictions have been removed.
6. ***Requests from authenticated data consumers*** – requests from authenticated data consumers will be limited to reading public metadata and data as well as reading restricted resources for which they have been granted authorization. New services supporting create, update, or delete operations on data resources will be limited to authenticated users.
7. ***Data access requests and user identity information must be passed through web services*** – the CUAHSI HIS is a distributed Services Oriented Architecture (SOA) with many different HydroServers. Data is obtained through automated web service calls made on behalf of a data consumer by a client application. New functionality eventually to be supported by HydroServer involves passing create, update, or delete requests through the HydroServer web service interfaces. HydroServer services do not have a visual log-in interface. Because of this, data consumers must be able to identify themselves through web service calls.
8. ***It is desirable that data consumers be able to use a single set of credentials to access data across all HydroServers (e.g., single sign-on)*** – client applications like HydroDesktop will use credentials supplied by the user for both authentication and authorization purposes when accessing data resources on HydroServers. It follows that:
   1. ***User credentials must be reusable across hydroservers*** – because clients like HydroDesktop will request data from multiple HydroServers, it is required that one set of user credentials be used to access data from many HydroServers.
   2. ***User credentials must be globally unique*** – if user credentials are not globally unique, it would be possible for a person to be unable to get the same user name on every server. For example, a user creates an account with a user name of “jeff” on one HydroServer and then tries to create an account with a user name of “jeff” on another HydroServer only to find that there is already a user named “jeff.”
9. ***HydroServers must enable data consumers to request authorization to specific data resources*** – HydroServers must have functionality that enables users to request authorization to access data resources on that server. This may occur automatically through web service calls, or it may involve a web page interface where requests are logged.
10. ***Data authorization requests will require agreeing to a data access agreement*** – the data access agreement will specify the terms of data access that is granted.
11. ***HydroServers must enable data publishers to respond to authorization requests*** – HydroServers must have functionality that enables data publishers to grant access for specific data consumers who have made requests to access specific restricted data resources.
12. ***Authorization to access data resources is assigned on a HydroServer*** – all authorization information will be stored with the data resources on the HydroServer on which the data resource is hosted.
13. ***HydroServer administrators and data owners will set access permissions for data resources*** – HydroServer administrators and data owners are in charge of assigning access control permissions for data on their HydroServer.
14. ***For time series data, the granularity for access control will be at the series level*** – for time series data, a data object to which access can be granted will consist of a data series identified by the unique combination of Site, Variable, Method, Source, and QualityControlLevel (e.g., the results of a WaterOneFlow GetValues web service call). The system will enable setting separate access control restrictions for metadata and data (e.g., public metadata with restricted data). Because of this granularity, the following will be possible:
    1. Controlling access to both metadata and data separately
    2. Controlling access to data resources based on their version or quality control level
    3. Controlling access to data resources based on their age
    4. Controlling access to all series at a site
    5. Controlling access to all series for a variable
    6. Controlling access to all series within a database
15. ***HydroServers will log data access requests*** – logging of data access requests will occur on individual HydroServers. The following information will be collected:
    1. Who requested the data?
    2. What type of request was made (e.g., read, write, delete)?
    3. Which data resource was accessed?
16. ***HydroServers will be capable of transmitting data access log information to HIS Central*** – for purposes of maintaining statistics of the overall HIS system, each HydroServer will be capable of transmitting data access logs to HIS Central.
17. ***A HydroServer will have a single access control system that is independent of ODM*** – the access control system will be generic so that it can support access control on any digital object type on a HydroServer and not just data series stored in ODM databases.
18. ***The access control system will be built using existing functionality where possible*** – If at all possible, authentication and access control functionality will adopt and use existing 3rd party systems (e.g. OpenID, OpenAuth, or other existing systems).