Infrastructure Properties and Planning (IPP)
Data Access Policy
09/24/2015

Responsible Office: IPP Finance and Information Technology
Facilities Services Data Steward: Vice President, Kyu Whang

POLICY STATEMENT
IPP is committed to protecting its administrative data by managing access and utilizing this data in a manner that is consistent with the need for security and confidentiality. We always assume that IPP data is restricted unless otherwise stated. Therefore, IPP has developed and will maintain clear and consistent procedures for access to IPP administrative data.

REASON FOR POLICY
Access to and release of IPP restricted data must be governed by the IPP Data Steward as charged in University Policy 4.12, Data Stewardship and Custodianship.

RELATED UNIVERSITY POLICIES
- University Policy 4.12, Data Stewardship and Custodianship
- University Policy 5.1, Responsible Use of Electronic Communications
- University Policy 5.4.1, Security of Information Technology Resources
- University Policy 5.4.2, Security Incidents

DEFINITIONS
Data Administrator – An individual who has had authority delegated to them by the IPP Data Steward to grant access to electronic data.

Data Custodian – An individual who possesses or has access to electronic data. This includes downloading a dataset to a computer from a data warehouse.

Data Steward – An individual with the responsibility for coordinating the implementation of access to data through the establishment and of the definitions of data sets available for access and the development of policies and access procedures for those data sets.

External User - A user defined by the system administrator as external, i.e. a user granted access to systems but not defined as an internal user. Typically, these are customers.

IPP Role Management System – The main system for assigning access to data in IPP. This is accomplished by assigning users to Roles and giving permission to the Role to access certain data.

Internal User - A user defined by the system administrator as internal to IPP.

Legitimate Interest – A need for IPP data that arises within the scope of university employment and/or in the performance of authorized duties.

DATA CLASSIFICATIONS

- **Public** – Data that is open to anyone
- **Cornell Community** – Data that is available only to the Cornell community. This generally means that access is granted via Kerberos authentication to anyone with a valid Cornell NetID.
- **Confidential** – Data that is available only to specifically authorized individuals with a legitimate interest; including federally regulated data.
- **Restricted** – Data that is available only to specifically authorized individuals with a legitimate interest. This data is regulated by the division.

RESPONSIBILITIES

The **IPP Data Steward** will oversee the implementation of access to IPP data through the establishment and definition of data sets available for use and the access procedures for those data sets. The IPP Data Steward will make decisions on data classifications and release of data.

The **IPP Data Administrators** will grant appropriate access to electronic data. Data Administrators are also required to perform periodic audits of the security of the systems they are responsible for.

Data Custodians of IPP data are any individuals who possesses or have access to IPP electronic data; including downloading a dataset to a computer from a data warehouse or web site. Any IPP data that is downloaded and saved to a computer must be in an encrypted folder. Data Custodians will be required to annually certify that they require access to IPP data and that it is appropriated secured on their computer.

SECURITY SYSTEMS

There are several security systems in use to protect IPP data:

1. OBIEE/BRIO Models – Access to data warehouses in the university BRIO system is granted via permissions to files and folders through a CIT permit server. This is administered by CIT via requests from IPP Programming Services.
2. EBS (Utilities Data System) - EBS uses Windows Active Directory to control membership to the groups with access.
3. T2 FLEX (Transportation Information System) – Access to T2 FLEX. This is overseen by the Director of Transportation and administered by the T2 Systems Administrator.
4. IPP Role Management System – Access to all other IPP data is granted through the Role Management System (RMS). This can be accomplished through assigning appropriate permissions at the system, application, or table level. This is overseen by the Director of Information Technology and administered by IPP Programming Services.
5. Maximo Internal Security – Access to the Maximo system is granted through Maximo internal security. This is overseen by the Director of Information Technology and administered by the Manager of Programming Services.
6. Building Coordinators Table – This table provides access to the Coordinators Database to view floor plans, room use, and some ticket data. This is overseen by the Director of Information Technology and administered by the Facilities Customer Service Center.

POLICY INTERPRETATION and CHANGE REQUESTS

All requests for interpretation of this policy and requests for changes to this policy should be made to the Director of Information Technology.

REQUESTS FOR ACCESS

Users requesting access to IPP data, must fill out an access request form. The various forms are located at: http://computing.fs.cornell.edu/about/fsit_helprequest.cfm

SYSTEMS

Agile

- Has a proprietary security system containing user groups, along with user access permissions that are linked to user roles. Anyone can request an Agile user account but only an Enterprise user or Site Administrator can authorize the account and setup individual user permissions.
- Internal and external users are granted access privileges based on their role.

Document Archive

- Access granted through the Role Management System (RMS).
- Restricted data – access granted only to users with a legitimate interest

EPAR System

- Highly confidential
- Access only granted within the EPAR system to authorized users

EBS (Utilities Data System)

EBS includes the following access Levels:

- **Non-authenticated:** limited view only (via a web browser).
- **Authenticated Accounts Payable:** view/update accounts payable (PUP) meters information only.
- **Authenticated Accounts Receivable:** view/update accounts receivable (GUP) meters information only.
- **Power:** view/update access to all screens & data.
- **Admin:** set and update user security, set current month (roll over) and send Service Unit Billing (SUB) file to general ledger system.

Facilities Inventory System

- Read only access to floor plans and room use data is given to primary building coordinators as defined in the Coordinators database maintained by the Facilities Customer Service Center or granted on the basis of NetID and in the RMS.
- All users have read only access to the facility code and facility name information in the Facilities file.

Facilities Physical Needs Management System

- Access granted through the Role Management System (RMS).

Facilities Web Site Information

- Access granted through the Role Management System (RMS).

Maximo

- Read only access to data is given to primary building coordinators as defined in the Coordinators database maintained by the IPP Customer Service Center or granted on the basis of NetID and Facility code in a security table maintained by Facilities Inventory.
- Maximo application data access is controlled by the internal security groups set up within Maximo.

Maximo includes the following systems:

- Customer Service Ticketing System
- Inventory Management System
- Preventive Maintenance
- Emergency Lights
- Job Cost Employee Data

T2 FLEX (Transportation Information System)

- Access to the FLEX is managed by the application-internal security management system based on a user's role.

Web Services

The requesting unit must provide:

- Business Need
- Consuming Application Name and Description
- Requested Date of Availability of the Data (MM/DD/YYYY)
- Data Requested - Provide overview of the data that will be retrieved from each system that will be accessed. Specify batch or real-time access. Specify one-time or on-going. If ongoing, specify how often.

- Data Delivery mechanism - Specify how the data will be accessed (ex: web page, application)
- The constituent populations of output data to be delivered
- Security - Please describe how the data will be secured.