Penn
Facilities & Real Estate Services

EXHIBIT "C"

# Cyber Security Policy

## Division of Facilities and Real Estate Services

## 1. Introduction.

This Cyber Security Policy ("Policy) is a formal set of rules applicable to Vendor/Service Providers, including their agents and subcontractors as well as the employees of each of them (each a "User") who have access to the cyber secure network controlled by the University's Division of Facilities and Real Estate Services. This Policy (i) describes the technology and information assets that must be protected, (ii) identifies many of the threats to those assets and (iii) informs Users of (a) requirements for protecting the cyber secure network, including its technology and information, (b) the User's responsibilities and privileges, (c) the acceptable uses of those assets, (d) the rules regarding internet access, (e) limitations on a User's access privileges, (f) the process for addressing violations of the policy, and (g) procedures for responding to incidents that threaten the security of the University's computer systems and network. Failure to comply with this Policy is a basis for termination of the Vendor/Service Provider's contract.

## 2. What we are protecting.

All Users shall protect the technology and information assets of the University from unauthorized access, theft and destruction. The technology and information assets of the University include the following components:

- Computer hardware, CPU, email, web and application servers.
- System Software including operating systems, database management systems, and backup and restore software, and communications protocols.
- Application Software used by the various departments within the University. This includes custom written software applications, and commercial off-the-shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, switches, firewalls, private lines, and associated network management software and tools.

These elements are collectively referred to in this policy as "Technology and Information Assets"

## 3. User Responsibility

When making use of the University's Technology and Information Assets, Users are required to comply with the University Policies on Acceptable Use of Electronic Resources, http://www.upenn.edu/computing/policy/aup.html.

Key provisions of the policy include the following:

- User accounts on University computer systems may be used only for business of the University and not for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and may give rise to both criminal and civil liability.
- Users are responsible for protecting all confidential information used and/or stored on their accounts. This includes logon IDs and passwords. All Users are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons.
- Users shall not use the University's Technology and Information Assets to purposely engage in activity with the intent to: harass other Users; degrade the performance of the system; divert system resources for the User's own use; or gain access to University systems for which the User does not have authorization.
- Users shall report any breaches in the University's computer security, any incidents of misuse of the University's Technology and Information Assets or violations of this policy to their immediate supervisor, who shall report it to the University's Facilities and Real Estate Services IT designee.

## 3.1. Use of the Internet.

If a User gains access to the Internet through the University's Technology and Information Assets, such access shall be used only in connection with providing contracted services to the University. Permissible uses include communicating via electronic mail with suppliers and business partners, obtaining information relevant to, or other purposes relevant to, the User's services to the University.

Internet service may not be used for transmitting, retrieving or storing any communications (i) of a discriminatory or harassing nature (ii) which are derogatory to any individual or group, (iii) that are obscene or pornographic, (iv) that are defamatory or threatening in nature, or (v) that constitute "chain letters." In addition, the Internet is not to be used for any illegal purpose or for personal gain.

## 3.2. Monitoring Use of computer Systems.

The University has the right and capability to monitor electronic information created and/or communicated by persons using University computer systems and networks, including but not limited to email messages and usage of the Internet. It is not University policy or intent to continuously monitor all computer usage by Users of the University computer systems and network. However, Users should be aware that the University may monitor usage, including, but not limited to, patterns of Internet usage (e.g. site accessed, on-line length, time of day access), and User's electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and University policy.

## 4. Access Control.

A fundamental component of the Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network.

Each individual User is required to have a unique login ID and password in order to gain access to the University's Technology and Information Assets. The User's password is to be kept confidential and **must not** be shared with any third party, including management or supervisory employees. All Users must comply with the following rules regarding the creation and maintenance of passwords where technically feasible:

- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed every 90 days.
- User accounts will be locked after 4 failed logon attempts.
- Passwords must contain a minimum of (8) characters.

• The password must contain characters from at least three of the following four categories:

- English uppercase characters (A - Z)
- English lowercase characters (a - z)
- Base 10 digits (0 - 9)
- One special character ex:!@#

Users are not permitted to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users are not permitted to login as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Each User shall be required to fill out and sign a SCADA Access Authorization and Briefing Form in order to receive User Login IDs and passwords. User Login IDs and passwords will be deactivated as soon as possible upon expiration or termination of a Vendor/Service Provider's contract or if a User is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the University or Vendor/Service Provider.

A Vendor/Service Provider's Supervisors / Managers shall immediately and directly contact the University IT Manager to report change in user status that requires terminating or modifying employee login access privileges.

Users who forget their password must call the University's Facilities and Real Estate Services IT designee to have a new password assigned to their account. The User must identify himself/herself by name, User ID and the name of its Vendor/Service Provider employer, to the University's Facilities and Real Estate Services IT designee.

Users will be responsible for all transactions occurring during login sessions initiated by use of the User's password and ID. Users shall not login to the University's electronic resources and then allow another individual to use the logged on device or otherwise share access to the University's systems. Passwords that are shared by Users will be deactivated.

## 4.1. Connecting to Third Party Networks.

This policy is established to ensure a secure method of connectivity between Penn and all third-parties required to electronically exchange information with the University.

"Third-party" refers to Vendors/Service Providers (including the User), consultants and business partners doing business with the University, and other partners who have a need to exchange information with the University. Third-party network connections are to be used only by the employees of the third-party and only for purposes related to performing a Vendor/Service Provider's responsibilities under its contract with the University. The third-party will ensure that only authorized Users will be allowed to access University information. The third-party will not allow Internet traffic or other private network traffic to flow into the University's network. This policy applies to all third-party connection requests and any existing third-party connections.

## 4.2. Connecting Devices to the Network.

Only authorized devices may be connected to the University network(s) on a case by case basis with approval from FRES IT. Authorized devices include but is not limited to PCs, workstations, and all other devices attached to the network that comply with the computer configuration guidelines of the University.

Users shall not attach devices to the network that are not authorized, owned and/or controlled by University. Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's. All devices must comply with the latest patches and virus definitions as applicable, and will be considered unauthorized unless so complying.

## 4.3. Remote Access.

Only authorized persons may remotely access the University network. Remote access is provided only to those employees, contractors and business partners of the University who have demonstrated a legitimate business need to exchange information with University systems through a secure ID. Users may not install software which provides remote access to the University's Technology and Information Assets unless authorized to remotely access the University network.

# 5. Data Privacy.

Users shall use University data only for the purpose of fulfilling contractual duties. Users shall not share such data with or disclose them to any third party without the prior written consent of the University of as otherwise required by law. By way of illustration and not of limitation,

User will not use such data for User's own benefit and, in particular, will not engage in "data mining" of University or end-user data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the University. All University or end-user data will be stored on servers, located solely within the Continental United States.

Vendors/Service Providers shall provide access to University data only to those employees and subcontractors who need to access the data to perform contractual obligations. Vendor's/Service Providers will ensure that employees and subcontractors who perform work under agreements with the University have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Policy, and have undergone appropriate background screening and possess all qualifications required by the University prior to being granted access to the University or end-user data.

Vendors/Service Providers shall ensure that post-interview or post-offer, pre-employment background checks are conducted as to all employees (i) performing any services at locations on the University's campus or (ii) who would have access to the University's technology and information assets, University data or end-user data. These checks shall include a federal criminal background check, state or county of residence criminal background checks for all jurisdictions where the individual has lived for the past seven (7) years, and a previous residential address search. The criminal background check shall include any criminal convictions as well as any periods of judicial oversight occurring within the last seven (7) years. Background checks shall include social security number trace and verification. Vendors/Service Providers shall review all background checks and shall exclude from participation in the performance of the Services any dishonest, dangerous or otherwise unqualified person.

Pre-employment background checks for any User shall be available to the University upon the University's request along with information regarding the analysis that Vendor/Service Provider performed when considering the information included in the background checks. The University will observe all relevant privacy laws in the handling and review of the reference and background checks. To the extent authorization is required from the employee in order to share reference and/or background checks with the University, Service Provider shall be responsible for obtaining such authorization. In discharging its responsibilities under this section, Vnedor/Service Provider shall comply with and abide by all applicable laws including, but not limited to, the Fair Credit Reporting Act, Title VII of the Civil Rights Act of 1964 and the Philadelphia Fair Criminal Records Screening Standards Ordinance.

## 6. Data Security and Integrity.

All facilities used to store and process University data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's/Service Provider's own data of a similar type, and in no event less than reasonable, taking into account the type and nature of the data involved. Without limiting the foregoing, Vendor/Service Provider warrants that all University data will be encrypted in transmission (including via web interface) at no less than 128-bit level encryption. To the extent that Vendor/Service Provider records, including records of its services, (such as work orders) include University data, Vendor/Service Provider shall securely store such data in accordance with this section.

This Policy is intended to meet the NIST 800-53 series of standards, including the best practices for information security management, and standards for the establishment, implementation, control, and improvement of the information security management systems, and is more fully expressed in the following University policy directives, copies of which are available to Vendor/Service Provider from the University's Facilities and Real Estate Services IT designee:

- Policy Directive on Access Authentication and Authorization
- Policy Directive on Audit and Accountability
- Policy Directive on Configuration Management and Change Control
- Policy Directive on Maintenance
- Policy Directive on Media Protection
- Policy Directive on Incident Response Plan

Users acknowledge that the User's compliance with this Policy is intended to meet these standards and directives, and Users shall not knowingly or negligently deviate from these standards and directives. User will provide to the University's employees and consultants, information reasonably requested by the University regarding Vendor's/Service Provider's security practices and policies. Vendor/Service Provider will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement. Vendor/Service Provider will implement commercially reasonable measures, including regular data integrity audits, to protect University data against deterioration or degradation of data quality and authenticity.

Vendor/Service Provider will at its own expense conduct or have conducted at least annually an audit in compliance with audit standard SSAE 16 SOC 2 of Vendor/Service Provider's security policies, procedures and controls resulting in the issuance of a Service Auditor's Report Type II.

Vendor/Service Provider will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement

## 7. Auditing.

In addition to providing results of the tests and procedures described above, the Vendor/Service Provider shall also submit to audits conducted by University personnel or by third parties engaged by the University for any other reasonable purpose as determined by University, including audits of:

- Practices and systems
- General controls and security practices and procedures,
- Disaster recovery and back up, procedures
- The Vendor/Service Provider's practices in complying with regulatory requirements,
- Any certification made by the Vendor/Service Provider.

The Vendor/Service Provider shall provide full cooperation to such auditors, inspectors, regulators, and representatives, including the installation and operation of audit software.

## 8. Training.

The Vendor/Service Provider shall provide training to all Users with respect to each User's responsibilities relative to cyber security. Such training must be sufficient to ensure each User's competence in cyber security to a level commensurate with his or her assigned job functions. Cyber security training may be obtained free of charge from the FBI and from the Department of Homeland Security via their respective websites.

## 9. Response to Legal Orders, Demands or Requests for Customer Data or End User Data.

Except as otherwise expressly prohibited by law, Vendor/Service Provider will:

- immediately notify University of and provide to the University a copy of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking University Data and/or End User Data;
- consult with University before providing a response;
- cooperate with University's reasonable requests in connection with efforts by University to intervene and quash or modify the legal order, demand or request; and
- Upon University's request, provide University with a copy of its response.

If the University receives a subpoena, warrant, or other legal order, demand or request seeking University Data or End User Data maintained by Vendor and not accessible by the University, the University will promptly provide a copy to Vendor/Service Provider. Vendor/Service Provider will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University's reasonable requests in connection with its response.

## 10. Data Compromise Response.

Immediately upon becoming aware of a data compromise, or of circumstances that could have resulted in unauthorized access to or disclosure or use of University Data, Vendor/Service Provider will notify the University, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Vendor/Service Provider shall immediately take all reasonable steps to mitigate the consequences of the Data Compromise and shall promptly take all corrective action necessary to prevent a future Data Compromise or creation of circumstances that could result in unauthorized access to or disclosure of University Data. Except as otherwise required by law, Vendor/Service Provider will not provide notice of the incident directly to the persons whose data were involved, regulatory agencies, or other entities, without prior written permission from University.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to University under law or equity, Vendor/Service Provider will reimburse University in full for all costs incurred by University in investigation and remediation of such Data Compromise, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract; the offering of 12 months' credit monitoring to each person whose data were compromised; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Compromise.