Revision #	2.2
Revision Date	August 2016
Policy Owner	Office of Information Security
Approved	9/19/2016

Acceptable Use Policy

1. Overview

Park University and the Office of Information Security are committed to protecting Park's students, employees, partners and the university confidential information and information system from illegal or damaging actions by individuals, either knowingly or unknowingly, while maintaining a culture of openness, trust and integrity.

Internet/Intranet/Extranet-related systems including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, Virtual Applications, and VPN are the property of Park University. These systems are to be used for business purposes serving the interests of the university and of our clients in the course of normal business operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Park University student, employee, and affiliate who handles information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of information technology system at Park University. These rules are in place to protect the students, employees, and the university. Inappropriate use exposes Park University to risks including malware attacks, compromise of network systems and services, as well as potential legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Park University business or interact with internal networks and business systems, whether owned or leased by Park University, the employee, or a third party. All students, employees, contractors, consultants, temporary, and other workers at Park University are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Park University policies and standards, along with federal and state laws and regulations.

This policy applies to students, employees, contractors, consultants, temporary employees, and other workers at Park University, including all personnel affiliated with third parties. This policy applies to all information technology systems that are owned or leased by Park University at any location including virtual locations.

4. Policy

4.1 General Use and Ownership

4.1.1 Park University proprietary information stored on electronic and computing devices whether owned or leased by Park University, the employee or a third party, remains the sole property of Park University. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Classification and Protection Policy.

4.1.2 Every user has the responsibility to promptly report the theft, loss, or unauthorized disclosure of Park University proprietary information.

4.1.3 Users may access, use, or share Park University proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use. If there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Park University may monitor equipment, systems, and network traffic at any time.

4.1.6 Park University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure access, is prohibited.

4.2.2 User must lock the screen of all computing devices or log off when the device is unattended.

4.2.3 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. For example, the systems administration staff may have a need to disable the network access of a host if that host is disrupting production services.

Under no circumstances is a Park University student or university employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Park University-owned resources.

The list below is by no means exhaustive, but an attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or university protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by Park University.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Park University or the end user does not have an active license.

3. Accessing data, a server or an account for any purpose other than conducting Park University business, even if you have authorized access.

4. Exporting software, technical information, encryption of software or technology, in violation of international or regional export control laws is illegal. Appropriate management should be consulted prior to export of any material that is in question.

5. Intentional introduction of malicious programs into the network or server such as viruses, worms, Trojan horses, e-mail bombs, etc.

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a Park University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any Park University account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to the Office of Information Security is made by sending an email to infosec@park.edu stating the reason for the port scanning and the target system or network.

12. Executing any form of network monitoring which will intercept data not intended for the student or employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network, or account.

14. Introducing honeypots, honeynets, or similar technology on Park University network.

15. Interfering with or denying service to any user other than the employee's host, for example, denial of service attack.

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, Park University students or employees to parties outside Park University without authorization from the information security office or Executive Staff.

4.3.2 Email and Communication Activities

When using university resources to access and use the Internet, users must realize they represent the university. Whenever employees state an affiliation to the university, they must also clearly indicate that the opinions expressed are their own and not necessarily those of the university. Questions may be addressed to the department of Information Technology Services (ITS) at helpdesk@park.edu

1. Sending unsolicited email messages, including the sending of junk mail or other advertising material to individuals who did not specifically request such material such as email spam.

2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding chain letters, Ponzi, or other pyramid schemes of any type.

6. Use of unsolicited email originating from within Park University's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Park University or connected via Park University's network.

4.3.3 Social Media

1. Use of social media by employees, whether using Park University's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Park University's systems to engage in social media activities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Park University's policy, is not detrimental to Park University's best interests, and does not interfere with an employee's regular work duties. Access to social media sites from Park University's systems is also subject to monitoring.

2. Park University's Confidential Information Policy also applies to social media activities. As such, employees are prohibited from revealing any university, confidential, or proprietary information when using social media.

3. Employees shall not engage in any social media activities that may harm or tarnish the image, reputation, and/or goodwill of Park University and/or any of its employees.

4. Employees may also not attribute personal statements, opinions or beliefs to Park University when using social media. If an employee is expressing his or her beliefs and/or opinions in social media posts, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Park University. Employees assume any and all risk associated with social media use.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Park University's trademarks, logos and any other Park University intellectual property may also not be used in connection with any social media activity.

5. Policy Compliance

5.1 Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by Park University InfoSec Office or Executive Staff in advance.

5.3 Non-Compliance

Violation of this policy may result in termination or suspension of access, in whole or in part, to Park University information systems at the discretion of ITS where such actions are reasonable to protect the University or the University information infrastructure. Any violation of this policy by a Park University student is also subject to the ramifications outlined in the Student Code of Conduct.

6. Related Standards, Policies and Processes

- Data Classification and Protection Policy
- Password Policy

If you have any questions regarding this policy, or any other Park University IT policy, please contact Information Security office at: infosec@park.edu

Defined Terms

Access Control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Access Control List: A means of determining the appropriate access rights to a given object given certain aspects of the user process that is requesting them, principally the process's user identity.

Algorithm: A finite set of well-defined instructions for accomplishing some task.

Anti-Virus Software: Computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software.

Authorized Use: The use of the university information technology network by any person who is authorized to do so by the university within the limits of that person's authorization, and as described in and permitted by the University Information Technology Policies and Procedures.

Authorized User(s): Any person authorized by the university to use the university's information technology network including, but not limited to: faculty, staff, students, and guests.

Backup: The process of periodically copying all of the files on a computer's disks onto a magnetic tape or other removable medium.

Certificate: A set of security-relevant data issued by a trusted third party organization, together with security information which is used to provide the integrity and data origin authentication services for the data (Security Certificate).

Chain Email: A term used to describe Emails that encourage you to forward them on to someone else.

Change Management: The process of developing a planned approach to change in an organization.

Cipher: A private alphabet, system of characters, or other mode of writing, contrived for the safe transmission of secrets.

Console Access: Communicating with an information technology resource through a locally-connected device, such as a keyboard / pointer device / monitor combination.

Database: Any set of information may be called a database. In this context, the term refers to computerized data, represented as an information set with a regular structure.

Decryption: The reverse of encryption by which the encrypted text is transformed to the readable text.

De-militarized Zone (DMZ): Any un-trusted network connected to, but separated from, the university's Information Technology Network by a firewall, used for external (Internet/partner, etc.) access from within the university, or to provide information to external parties.

Denial of Service (DoS): An attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by overloading the computational resources of the victim system.

Data Encryption Standard (DES): A method for encrypting information selected as an official Federal Information Processing Standard for the United States, and which has enjoyed widespread use internationally, but is now considered to be insecure for many applications.

Domain Name System (DNS): A system that stores information about computer and network names in a kind of distributed database on networks, such as the Internet.

Email: The electronic transmission of information through a mail protocol such as SMTP.

Email Bomb: Causing a user's Email account to reach maximum storage capacity by through the excessive sending of Email messages for the sole purpose of being malicious.

Encryption: The process of making data unreadable to unauthorized entities by applying a cryptographic algorithm (an Encryption Algorithm).

Extranet: An interconnection between two or more organizations in order to create a private network to share information.

File Transfer Protocol (FTP): A software standard for transferring computer files between machines with widely different operating systems.

Firewall: A piece of hardware or software which functions in a networked environment to prevent some communications forbidden by the network policy. It has the basic task of preventing intrusion from a connected network device into other networked devices.

Forwarded Email: Email explicitly redirected from one account to another.

Guest User: Any visitor to the university, not including faculty, staff, or students, who is properly authorized to use the university Information Technology Network.

Hardware: The physical, touchable, material parts of a computer or other system. The term is used to distinguish these fixed parts of a system from the more changeable software or data components which it executes, stores, or carries.

HyperText Transfer Protocol (HTTP): The primary method used to communicate information on the World Wide Web.

Host: Any computing device attached to a computer network.

Information Security: Information Security is the part of Information Technology Services that is responsible for coordinating and overseeing campus wide compliance with university policies and

procedures regarding the confidentiality, integrity, and security of its information assets.

Information Security Awareness Initiative: An educational initiative developed by Information Security that will train Authorized Users about the University Information Technology Policies and Procedures and how to stay in compliance with them. This will include, but is not limited to, teaching classes, sending alerts and reminders, and writing guidelines.

Information Security Guidelines: (in development) Attached to these policies are guidelines that help the user comply with the policies.

Instant Messaging: An on-line communication service in which conversations happen in real time, and the "on-line status" between users is conveyed such as if a contact is actively using the computer.

Intellectual Property: A form of legal entitlement which allows its holder to control the use of certain intangible ideas and expressions.

Internet: The publicly available worldwide system of interconnected computer networks.

Internet Protocol (IP) Address: A unique number used by machines (usually computers) to refer to each other when sending information through the Internet.

IP Security (IPSec): A standard for securing Internet communications by encrypting and authenticating all data.

Log: A chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event (also known as an audit trail).

Malicious Software (malware): Any software developed for the purpose of doing harm to a computer system.

Mass Emailing: An Email that is sent to a group of individuals.

Network: A system for communication among two or more computers.

Network Drive: A computer storage medium accessible from a network connection.

Network Sniffing: The act of watching Internet Protocol packets as they traverse a local network.

Operating System (OS): The system software responsible for the direct control and management of hardware and basic system operations, as well as running application software.

Packet Spoofing: To capture, alter, and retransmit a communication stream in a way that misleads the recipient.

Pass-phrase: A collection of 'words' used for access control, typically used to gain access to a computer system.

Patch: An update to an existing piece of software that corrects errors or adds new features (also known as a hot-fix).

Phishing: The act of sending Email for the purpose of surrendering private information that will be used for identity theft.

Ping: Slang term for a small network message sent by a computer to check for the presence and alertness of another computer.

Pretty Good Privacy (PGP): A computer program which provides cryptographic privacy and authentication.

Principle of Least Access: A user must have access to the resources necessary to accomplish a given task, but not to resources unnecessary for completing the task, thus minimizing potential security risks.

Proprietary Information: Information on the university network that is owned by the university, a form of intellectual property.

Protocol: A convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints.

Remote Access: Communicating with an information technology resource from different location.

Restoration: Action taken to repair and return to service one or more information technology resources that have a degraded quality of service or have a service outage.

Risk Analysis: A process to ensure that the security controls for a system are fully commensurate with its risks.

Risk Assessment: The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.

Scanning: Checking for services presented on networks, usually as part of a cracking attempt or computer security scan.

Secure Channel: A communication that uses strong encryption.

Secure Shell (SSH): Both a computer program and an associated network protocol designed for logging into and executing commands on a remote computer. It provides secure encrypted communications between two untrusted hosts over an insecure network

Secure Sockets Layer (SSL): A cryptographic protocol to provide secure communications on the Internet.

Security: The term “Security” is used in the sense of minimizing the vulnerabilities of assets and resources.

Security Audit: This function provides monitoring and collection of information about security related actions, and subsequent analysis of the information to review security policies, controls, and procedures.

Security Guideline: A guideline is a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended.

Security Policy: A policy is a document that outlines specific requirements or rules that must be met.

Security Standard: A standard is a collection of system-specific or procedural-specific requirements that must be met by everyone.

Sensitive Information: Information is considered sensitive if it can be damaging to university or its reputation.

Service Set Identifier (SSID): A code attached to all data on a wireless network to identify the data as part of that network.

SPAM: Unauthorized or unsolicited electronic mailings.

Student(s): Person(s) enrolled in at least one credit class at the university.

Threat: A potential violation of security.

Traffic Flooding: To send an excessive amount of traffic to an information technology resource, causing a Denial of Service attack.

Trojan Horse: Malicious software that is disguised as legitimate software.

Trust Relationship: A relationship between two networks that enables a user in one network to access resources in the other.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people, both inside and outside the university, who are not authorized to know that information.

Unauthorized Use: Use of the university network by unauthorized users in violation of the law or in violation of the University Information Security Policies and Procedures.

Unauthorized Users: Use of the university network who are not authorized users, or use of the university information technology network in violation of the law or in violation of the University Information Technology Policies and Procedures.

University: The Board of Trustees of Park University, a Missouri nonprofit organization that does business as "Park University."