Last updated: *June 24, 2016*
March 1, 2019

Network Protection and Information Security Policy

PURPOSE

The purpose of this policy is to establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of Pikes Peak Regional Building Department information handled by computer networks and information systems, or otherwise collected and maintained by Pikes Peak Regional Building Department electronic document(s) during the course of business that contain personal identifying information.

SCOPE

This policy applies to all who access Pikes Peak Regional Building Department computer networks. Throughout this policy, the word “user” will be used to collectively refer to all such individuals. This policy also applies to all computer networks and information systems owned by or administered by Pikes Peak Regional Building Department or its partners.

POLICY

All information traveling over Pikes Peak Regional Building Department computer networks and information systems that has not been specifically identified as the property of other parties will be treated as though it is a Pikes Peak Regional Building Department asset. It is the policy of Pikes Peak Regional Building Department to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of Pikes Peak Regional Building Department to protect information belonging to third parties, entrusted to Pikes Peak Regional Building Department, in a manner consistent with its sensitivity and in accordance with any and all applicable agreements.

RESPONSIBILITIES

The Information Technology (IT) Director is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide computer networks and information systems security policies, standards, guidelines, and procedures. While responsibility for computer networks and information systems on a day-to-day basis is every employee's duty, the specific guidance, direction, and authority for computer networks and information systems is centralized in the IT department for all of Pikes Peak Regional Building Department. This department will perform information systems risk assessments, prepare information systems security action plans, evaluate information systems security products, and perform other activities necessary to assure a secure information systems environment.

The Network administrator is responsible for coordinating investigations into any alleged computer networks or information systems security compromises, incidents, or problems with the IT infrastructure. All compromises or potential compromises must be immediately reported to the IT department. The Network administrator is responsible for contacting the IT Director. All members of the IT department are responsible for reporting all suspicious computer or network security related activities to the Network administrator or IT Director. The Network administrator also implements the requirements of this and other computer networks and information systems security policies, standards, guidelines, and procedures.

The IT Director and IT department supervisors are responsible for ensuring that appropriate computer networks and information systems security measures are observed by users in their respective departments. In addition to allocating sufficient resources and staff time to meet the requirements of these policies, the IT Director and department supervisors are responsible for ensuring that all employee users are aware of Pikes Peak Regional Building Department policies related to computer networks and information systems security.

Users are responsible for complying with this and all other Pikes Peak Regional Building Department policies defining computer networks and information systems security measures. Users are also responsible for bringing all known information security vulnerabilities and violations that they notice to the attention of the IT department.

SYSTEM ACCESS CONTROL

End-User Passwords

Pikes Peak Regional Building Department has an obligation to effectively protect the intellectual property and personal and financial information entrusted to it by customers, employees, partners and others. Using passwords that are difficult to guess is a key step toward effectively fulfilling that obligation.

Any password used to access information stored and/or maintained by Pikes Peak Regional Building Department must be at least eight (8) characters long, contain at least one (1) uppercase letter, one (1) lowercase letter, and one (1) number or special character.

Passwords will expire every six (6) months. When a password expires or a change is required, users should create a new password that is not identical to the last three (3) passwords previously used.

Passwords stored electronically may not be stored in readable form where unauthorized persons might discover them.

Passwords may not be written down and left in a place where unauthorized persons might discover them.

Passwords may never be shared or revealed to anyone other than authorized user(s).

If a password is suspected of being disclosed or known to have been disclosed to anyone other than authorized user(s), it should be changed immediately.

Password System Set-Up

All computers permanently or intermittently connected to Pikes Peak Regional Building Department local area networks must have password access controls. If the computers contain confidential or protected information, an extended user authentication system approved by the IT department may be required. Multi-user systems (servers) should employ user IDs and passwords unique to each user and user privilege restriction mechanisms with privileges based on an individual's need-to-know. Network-connected, single-user systems must employ hardware or software controls approved by the IT department that prevent unauthorized access.

All vendor-supplied default fixed passwords, if any, must be changed before any computer or communications system is used in production. This policy applies to passwords associated with end-user IDs and passwords associated with privileged user IDs.

Where systems software permits it, the number of consecutive attempts to enter an incorrect password must be strictly limited. After five (5) unsuccessful attempts to enter a password, the involved user ID must be suspended until reset by the Network administrator or temporarily disabled for no less than fifteen (15) minutes.

Whenever information system security has been compromised or if there is a reason to believe that it has been compromised, the involved Network administrator must immediately take measures to ensure that passwords are properly protected. This may involve resetting all user passwords and requiring users to change them prior to next system log on.

Whenever information system security has been compromised or if there is a reason to believe that it has been compromised, the involved Network administrator must take measures to restore the system to secure operation. This may involve reloading a trusted version of the operating system and all security-related software from trusted storage media or original source-code disks/sites. The involved system then would be rebooted. All changes to user privileges taking effect since the time of suspected system compromise must be reviewed by the Network administrator for unauthorized modifications.

Logon and Logoff Process

All users must be positively identified prior to being able to use any Pikes Peak Regional Building Department distributed computer network or information system resources. Positive identification for internal Pikes Peak Regional Building Department networks involves a user ID and password, both of which are unique to an individual user or an extended user authentication system.

Positive identification for all Internet and remote lines involves the use of an approved, extended user authentication technique. The combination of a user ID and fixed password does not provide sufficient security for Internet or remote connections to Pikes Peak Regional Building Department systems or networks. Modems, wireless access points, routers, switches or other devices attached to network-connected workstations located in Pikes Peak Regional Building Department offices are forbidden unless they meet all technical requirements and have a user authentication system approved by the IT department.

The logon process for network-connected Pikes Peak Regional Building Department computer systems must simply ask the user to log on, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters may not be provided until a user has successfully provided both a valid user ID and a valid password.

If there has been no activity on a computer terminal, workstation, or personal computer for a certain period of time, the computer networks and information systems should automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period of time of inactivity should not exceed fifteen (15) minutes. An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room badge readers, or similar technology.

With the exception of electronic check in kiosks or other systems where all regular users are anonymous, users are prohibited from anonymously logging into any Pikes Peak Regional Building Department computer networks and information systems or network. If users employ systems facilities that permit them to change the active user ID to gain certain privileges, they must have initially logged on employing a user ID that clearly indicates their identity or affiliation.

SYSTEM PRIVILEGES

Limiting System Access

The computer networks and information systems privileges of all users, systems, and independent operating programs such as agents, must be restricted based on the need-to-know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

Default user file permissions must not automatically permit anyone on the system to read, write, execute or delete a system file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions are prohibited. Default file permissions are granted to limited groups of people who have a genuine need to know.

Users with personally-owned computers are responsible for administering a screen saver program securing access to their machine's hard disk drive and setting passwords for all applications and systems software that provide the capability of connecting to Pikes Peak Regional Building Department resources. Use of personally-owned computers on the network is discouraged.

Pikes Peak Regional Building Department computer networks and information systems must restrict access to the computers that users can reach over Pikes Peak Regional Building Department networks. These restrictions can be implemented through routers, gateways, firewalls, wireless access points, and other network components. These restrictions must be used to, for example, control the ability of a user to log on to a certain computer then move from that computer to another.

Process for Granting System Privileges

Requests for new user IDs and changed privileges must be in writing and approved by the user's supervisor before the Network administrator fulfills these requests. Documents or emails reflecting these requests must be retained for a period of at least one (1) month.

Individuals who are not Pikes Peak Regional Building Department employees or partners may not be granted a user ID or be given privileges to use Pikes Peak Regional Building Department computers or networks unless the written approval of a sponsoring department head has been obtained, and the employee agrees to full responsibility for all activities carried out by the individual(s) she or he is sponsoring. This can be accomplished by contacting the IT Director.

Privileges granted to users who are not Pikes Peak Regional Building Department employees must be limited to periods of one hundred eighty (180) days or less. As needed, users who are not Pikes Peak Regional Building Department employees must have their privileges reauthorized by the sponsoring department head every one hundred eighty (180) days.

Special privileges, such as the default ability to write to the files of other users, must be restricted to the IT department. An exception to this policy may be made if there is justified business and permission is acquired from the sponsoring department head. Configuration changes, operating system changes, and related activities that require system privileges must be performed by the Network administrator.

Third-party vendors must not be given Internet or remote privileges to Pikes Peak Regional Building Department computers or networks unless the Network administrator or IT Director determines that they have a legitimate business need. These privileges must be enabled only for the time period required to accomplish the approved tasks, such as remote maintenance. If a perpetual or long-term connection is required, then the connection must be established by approved, extended user authentication methods.

All users wishing to use Pikes Peak Regional Building Department internal networks, or multi-user systems that are connected to Pikes Peak Regional Building Department internal networks, signify their agreement to comply with all applicable policies by their logon to the network.

Process for Revoking System Access

All user IDs will have the associated privileges revoked after a certain period of inactivity not exceeding one hundred and eighty (180) days.

If a computer or communication system access control subsystem is not functioning properly, it should default to denial of privileges to users. If access control subsystems are malfunctioning, the systems should remain unavailable until such time as the problem has been rectified.

Users must not test or attempt to compromise computer networks or information systems security measures unless specifically approved in advance and in writing by the IT Director. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered serious violations of Pikes Peak Regional Building Department policy. Customer requests that Pikes Peak Regional Building Department security mechanisms be compromised must not be satisfied unless the IT Director approves in writing, in advance, or Pikes Peak Regional Building Department is compelled to comply by law. Short-cuts bypassing computer networks or information systems security measures, pranks, and practical jokes involving the compromise of computer networks or information systems security measures are absolutely prohibited.

The privileges granted to users, based on their role within the organization, should be reevaluated by administration annually. In response to feedback from building officials, department supervisors, the Human Resources department, or the IT Director, Network administrators must promptly revoke all privileges no longer needed by users.

Department supervisors must promptly report all significant changes in employee duties or employment status to the IT department or Network administrators responsible for user IDs associated with the involved persons. For all terminations, the department supervisor must issue a request of status change to the IT department and all Network administrators who might be responsible for a system on which the involved employee might have a user ID.

Establishment of Access Paths

Changes to Pikes Peak Regional Building Department internal networks include loading new software, changing network addresses, reconfiguring routers, and adding remote lines. With the exception of emergency situations, all changes to Pikes Peak Regional Building Department computer networks or information systems must use the formal change management process and be documented in a work order request. In addition, the Request for Change (RFC) must be approved in advance by the IT Director, except that delegated emergency changes to computer networks or information systems must be made by persons who are authorized by the IT department. This process prevents unexpected changes from leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees, but also to vendor personnel.

Employees must not establish electronic bulletin boards, local area networks, FTP servers, web servers, modem connections to existing local area networks, illegal peer-to-peer sharing, or other multi-user systems for communicating information, without the specific approval of the IT Director. New types of real-time connections between two or more in-house computer systems must not be established unless such approval is obtained.

Participation in external networks as a provider of services that external parties rely on is prohibited, unless Pikes Peak Regional Building Department legal counsel has identified the legal risks involved and the IT Director has expressly accepted these and other risks associated with the proposal.

Acquisition of technology services or relying on an external party for computer or network services is prohibited, unless Pikes Peak Regional Building Department legal counsel has identified the legal risks involved, the IT Director has expressly accepted these and other risks associated with the proposal, and the service provider meets the security and technology requirements identified by the IT department.

All Pikes Peak Regional Building Department computers that connect to an internal or external network must utilize password-based access controls or an extended user authentication system. Multi-user systems should employ software that restricts access to the files of each user, logs the activities of each user, and has special privileges granted to the Network administrator. Single-user systems should engage access control software, approved by the IT department, including boot control and an automatic screen blanker that are invoked after a certain period of no input activity. Portable computers and home/personally-owned computers containing Pikes Peak Regional Building Department information are also covered by this policy, as are network devices such as firewalls, gateways, routers, and bridges.

Remote maintenance ports for Pikes Peak Regional Building Department computer networks or information systems must be disabled until the time they are needed by the vendor. These ports must be disabled immediately after use.

Portable devices (smartphones, tablet computers, etc.) using Wi-Fi or commercial data networks should not be used for data transmissions containing confidential personal information, unless the connection is encrypted. Such links may be used for electronic communications as long as users understand that confidential personal information must not be transmitted using this technology.

COMPUTER VIRUSES, WORMS, AND TROJAN HORSES

Users must keep approved and current virus-screening software enabled on their computers. This software must be used to scan all software coming from third parties or other Pikes Peak Regional Building Department departments, and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

Users are responsible for damage occurring because of viruses on computer systems under their control. As soon as a virus is detected, the involved user must immediately contact the IT department to assure that no further infection takes place and that experts are promptly engaged to eradicate the virus.

All personal computer software should be copied prior to its initial usage, and such copies must be stored in a safe place. These master copies can be used for recovery from computer virus infections, hard disk crashes, and other computer problems.

Pikes Peak Regional Building Department computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software

vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a testing regimen approved by the IT Director or Network administrator.

Data and Program Backup

Personal computer users are responsible for backing up the information stored on the local drive of their computer. For multi-user computer (servers) and communication systems, the Network administrator is responsible for making regular backups.

To ensure that valuable or critical data is backed up, it must be stored on network servers managed by the IT department or a trusted partner.

Pikes Peak Regional Building Department requires the use of industry-standard media, techniques, and timelines in executing all backups. For multi-user computer systems, whenever systems software permits, backups must be performed without end-user involvement, over an internal network and outside regular business hours.

Storage of backup media is the responsibility of the user or Network administrator involved in the backup process. Backup media must be stored securely, and critical business information is to be stored in triplicate to include at least one (1) off-site backup location.

Retention of information located within the computer networks or information systems will be determined by content and some information will not be retained indefinitely. Financial data and information, to include database records, are to be retained for a period of no less than seven (7) years. Transactional business information such as any record related to the purchase of services, shall be retained indefinitely. Other information must be properly disposed of when no longer needed, which is generally within thirty (30) days of deletion or notification of disposal. Individual users of Pikes Peak Regional Building Department are responsible for information retention that only relates to and is in the control of the individual user.

Department supervisors are responsible for preparing, testing, and periodically updating department contingency plans to restore service for all non-IT managed production applications and systems. The IT department is responsible for preparing, testing, and periodically updating network service contingency plans.

All Confidential information stored on backup media should be encrypted using approved encrypting methods.

Portable Computers

Employees in the possession of portable, laptop, notebook, handheld, tablet and other transportable computers containing Confidential information must not leave these computers unattended at any time unless the information is stored in encrypted form.

Whenever Confidential information is written to a disk or other storage media, the storage media should be suitably marked as confidential. When not in use, this media should be stored in a locked safe, locked furniture, or a similarly secured location.

REMOTE PRINTING

Printers must not be left unattended if Confidential information is being printed or soon will be printed. The persons attending the printer must be authorized to examine the information being printed.

Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

PRIVACY

Unless contractual agreements dictate otherwise, messages sent over Pikes Peak Regional Building Department computer networks and information systems are the property of Pikes Peak Regional Building Department. Administration reserves the right to examine all data stored in or transmitted by these systems. Because Pikes Peak Regional Building Department computer networks and information systems are to be used for business purposes, users are to have no expectation of privacy associated with the information they store in or send through these systems.

When providing computer-networking services, Pikes Peak Regional Building Department does not provide default message protection services such as encryption. No responsibility is assumed for the disclosure of information sent over Pikes Peak Regional Building Department networks, and no assurances are made about the privacy of information handled by Pikes Peak Regional Building Department internal networks. In those instances where session encryption or other special controls are required, it is the user's responsibility to ensure that adequate security precautions have been taken. Nothing in this paragraph must be construed to imply that Pikes Peak Regional Building Department policy does not support the controls dictated by agreements with third parties, such as organizations that have entrusted Pikes Peak Regional Building Department with Confidential information.

Control of Personal Information

At any time, while accessing Pikes Peak Regional Building Department network(s), any user while online may decline participation in any activity that asks for information (i.e. survey or e-mail). The user's choice not to participate will in no way affect the user's ability to use any other feature on Pikes Peak Regional Building Department network(s). In online applications that ask for personal information, user(s) also are provided the option of canceling or "clearing all fields" of information and terminating the application prior to saving or submitting such application(s).

Use of Cookies

To better serve Pikes Peak Regional Building Department users, Pikes Peak Regional Building Department may use "cookies" to customize the user(s) browsing experience. Cookies are simple text files stored on the user(s) computer by the user(s) web browser. They provide a method of distinguishing among visitors to Pikes Peak Regional Building Department network(s).

Cookies created on the user(s) computer by using Pikes Peak Regional Building Department network(s) do not contain personally identifiable information and do not compromise the user(s) privacy or security. Visitors may delete the cookie file by using any of the widely available methods. Use of cookies is required in order to access pprbd.org.

LOGS AND OTHER SYSTEMS SECURITY TOOLS

Every distributed computer network and information system must include sufficient automated tools to assist the Network administrator in verifying a system's security status. These tools must include mechanisms for the recording, detection, and correction of commonly-encountered security problems.

To the extent that systems software permits, computer networks and information systems which handle sensitive, valuable, or critical Pikes Peak Regional Building Department information, must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges, and changes to logging system configurations.

Logs containing computer networks and information systems security-relevant events must be retained for at least three (3) months. During this period, logs must be secured such that they cannot be modified, and such that only authorized persons can read them.

Certain information must be captured whenever it is suspected that computer or network-related crime or abuse has taken place. The relevant information must be securely stored off-line until such time as it is determined that Pikes Peak Regional Building Department will not pursue legal action or otherwise use the information. The information to be immediately collected includes the computer networks and information systems logs, application audit trails, other indications of the current system states, and copies of all potentially involved files.

Although Network administrators are not required to promptly load the most recent version of operating systems, they are required to promptly apply all security patches to the operating system that have been released by knowledgeable and trusted user groups, well-known systems security authorities, or the operating system vendor. Only those systems security tools supplied by these sources or by commercial software organizations may be used on Pikes Peak Regional Building Department computers and networks. Additionally, only vendor-supported versions of operating systems and applications should be used on production systems. This will generally require periodic upgrades to the current release or the most recent prior version.

HANDLING NETWORK SECURITY INFORMATION

From time to time, the IT Director will designate individuals to audit compliance with this and other computer networks and information systems policies. At the same time, every user must promptly report to the IT Director or his/her designee any suspected network security problem, including intrusions and out-of-compliance situations.

Provided that no intent to damage Pikes Peak Regional Building Department computer networks and information systems existed, if users report a computer virus infestation immediately after it is noticed, even if their negligence was a contributing factor, no disciplinary action should be taken.

All network or systems software malfunctions must be immediately reported to the IT department or the involved external service provider.

Information about security measures for Pikes Peak Regional Building Department computer networks and information systems is confidential and must not be released to people who are not authorized users of the involved systems, unless the permission of the IT Director has been obtained. For example, it is prohibited to publish system access information in directories.

INFORMATION SECURITY

Risk Identification and Assessment

Pikes Peak Regional Building Department intends to undertake efforts to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The IT Director will establish procedures for identifying and assessing such risks in each relevant area of operations, including:

- **Employee training and management.** The IT Director will coordinate with representatives in the Human Resources department to evaluate the effectiveness of procedures and practices relating to access to and use of financial records. This evaluation will include assessing the effectiveness of current policies and procedures in this area.

- **Information Systems and Information Processing and Disposal.** The IT Director will assess the risks to nonpublic financial information associated with information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. The IT Director will also assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- **Detecting, Preventing and Responding to Attacks.** The IT Director will evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies.

Designing and Implementing Safeguards

The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper, or other form. The IT Director will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers

The IT Director shall coordinate with those responsible for the third-party service procurement activities among the IT department and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of

maintaining appropriate safeguards for nonpublic financial information of customers and other third parties to which they will have access. These standards shall apply to all existing and future contracts entered into with such third-party service providers.

Adjustments to Policy

The IT Director is responsible for evaluating and adjusting this Network Protection and Information Security Policy based on the risk identification and assessment activities undertaken pursuant to the policy, as well as any material changes to the Pikes Peak Regional Building Department operations or other circumstances that may have a material impact on the policy.

Physical Security of Computer and Communications Gear

All Pikes Peak Regional Building Department network equipment must be physically secured. Access to data centers, telephone wiring closets, network switching rooms, and other areas containing Confidential information must be physically restricted.

All employees who must keep Pikes Peak Regional Building Department Confidential information offsite in order to do their work must securely store this information. At the time of separation from Pikes Peak Regional Building Department, all Confidential information must be returned immediately.

Exceptions

Pikes Peak Regional Building Department acknowledges that, under rare circumstances, certain users may need to utilize systems that are not compliant with these policies. All such instances must be approved in writing and in advance.

Violations

Pikes Peak Regional Building Department network users who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination and/or legal action.

Methods of Paper and Electronic Records Destruction

Paper and electronic documents shall be disposed of to ensure that all confidential and personal identifying information contained in the documents is rendered unreadable or indecipherable through any means.

“Personal identifying information” means a social security number, personal identification number, password, pass code, official state or government-issued driver’s license or identification card number, a government passport number, biometric data, as defined in C.R.S. § 24-73-103(1)(a), an employer, student or military identification number, or a financial transaction device, as defined in C.R.S. § 18-5-701(3).

For the destruction of paper documents containing confidential or personal identifying information, each department of Pikes Peak Regional Building Department is provided a bin for the destruction of such records. To prevent disclosure, the material in the bins is collected by a data-destruction/ shredding service provider. Such bin SHALL NOT be used to dispose of any records or materials that are not confidential or that do not contain personal identifying information. The data-

destruction/shredding service provider shall arrange for the destruction of the documents by shredding, erasing or otherwise modifying the confidential and personal identifying information.

For the destruction of electronic documents containing confidential or personal identifying information, each department of Pikes Peak Regional Building Department will work with the legal department and/or the IT department to arrange for such electronic documents to be erased, redacted, or otherwise modified to make the confidential and personal identifying information unreadable or indecipherable.

TERMS AND DEFINITIONS

Access control: A system to restrict the activities of users and processes based on the need to know.

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Algorithm: A mathematical process for performing a certain calculation. In the information security field, it is generally used to refer to the process for performing encryption.

Badge reader: A device that reads employee identity badges and interconnects with a physical access control system that may control locked doors.

Booting: The process of initializing a computer system from a turned-off or powered-down state.

Bridge: A device that interconnects networks or that otherwise permits networking circuits to be connected.

Computer Networks and Information Systems: Any and all network connected devices or software as well as any device containing information or data owned by or managed by Pikes Peak Regional Building Department. This extends to third-party hosting services that Pikes Peak Regional Building Department manages information or data.

Compliance statement: A document used to obtain a promise from a computer user that such user will abide by system policies and procedures.

Confidential information: A sensitivity designation for information, the disclosure of which is expected to damage Pikes Peak Regional Building Department or its partners.

Critical information: Any information essential to Pikes Peak Regional Building Department business activities, the destruction, modification, or unavailability of which would cause serious disruption to Pikes Peak Regional Building Department business.

Cryptographic challenge and response: A process for identifying computer users involving the issuance of a random challenge to a remote workstation, which is then transformed using an encryption process and a response is returned to the connected computer system.

Default file permission: Access control file privileges, read, write, execute, and delete, granted to computer users without further involvement of either a security administrator or users.

Default password: An initial password issued when a new user ID is created, or an initial password provided by a computer vendor when hardware or software is delivered.

Dynamic password: A password that changes each time a user logs on to a computer system.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

Encryption: A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives.

End User: An individual who employs computers to support Pikes Peak Regional Building Department business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process typically achieved by user IDs and fixed passwords, such as hand-held tokens and dynamic passwords.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have passed some security check, such as providing a password.

Front-end processor (FEP): A small computer used to handle communications interfacing for another computer.

Gateway: A computer system used to link networks that can restrict the flow of information and that employ some access control method.

Hand-held token: A commercial dynamic password system that employs a smart card to generate one-time passwords that are different for each session.

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the time frames that these types of information must be kept.

Isolated computer: A computer that is not connected to a network or any other computer. For example, a stand-alone personal computer.

Logon banner: The initial message presented to a user when he or she makes connection with a computer.

Logon script: A set of stored commands that can log a user onto a computer automatically.

Master copies of software: Copies of software that are retained in an archive and that are not used for normal business activities.

Multi-user computer system: Any computer that can support more than one user simultaneously.

Network administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password reset: The assignment of a temporary password when a user forgets or loses his or her password.

Password-based access control: Software that relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user ID: A user ID that has been granted the ability to perform special activities, such as a shutdown of a multi-user system.

Router: A device that interconnects networks using different layers of the Open Systems Interconnection (OSI) Reference Model.

Screen blanker or screen saver: A computer program that automatically blanks the screen of a computer monitor or screen after a certain period of inactivity.

Security patch: A software program used to remedy a security or other problem(s), commonly applied to operating systems, database management systems, and other systems software.

Sensitive information: Any information, the disclosure of which could damage Pikes Peak Regional Building Department or its business associates.

Shared password: A password known by or used by more than one individual.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges permitting the involved user or process to perform activities that are not normally granted to other users.

Suspending a user ID: The process of revoking the privileges associated with a user ID.

Terminal function keys: Special keys on a keyboard that can be defined to perform certain activities such as save a file.

User IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to Pikes Peak Regional Building Department or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.