

Policy and OP DEFINITIONS

1. Access – the ability to read, write, modify, or communicate data/information or otherwise use any system resource.
2. Access Controls – rules for limiting access to safeguard systems and data at all times and under all conditions.
3. Anti-Virus Coordinator – The person designated by the CTO to monitor and coordinate anti-virus activities within the DHHR.
4. Archive – (1) A long-term storage media, often on magnetic tape, for backup copies of files or files that are no longer in active use. (2) To move data to a less accessible or less expensive storage media or method.
5. Audit Controls – represent a set of procedures, policies, and record keeping activities that are established to ensure legal, ethical, and proper business practices.
6. Audit Log – Captures the computer user's actions while logged on to a system and saves the information to a database table or formatted file.
7. Authentication - Authentication refers to the verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by its claimed source. Authentication techniques usually form the basis for all forms of access control to systems and/or data.
8. Authorized Network Users – Individuals who have been granted access to DHHR network resources through an assigned userid.
9. Backup - To copy files from one storage area, especially a hard disk, to another to prevent their loss in case of a disk failure.
10. Back-up Files – Electronic files created to restore computer system files that have become inaccessible on a computer system.
11. Bandwidth - A measure of the amount of data that can be passed by a communication channel in a given amount of time.
12. Basic Input/Output System (BIOS) – A set of instructions and routines that enable the computer to communicate with the various devices in the system, such as memory, disk drives, keyboard, monitor, printer, and communication ports. The BIOS handles the flow of data between the operating system and the hardware.
13. Biometrics - A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).

14. Bureau Commissioners - Senior leaders who report directly to the Secretary of the DHHR and manage various Bureaus of DHHR, (i.e. the OIG and the Bureaus for Public Health, Children and Families, Behavioral Health and Health Facilities, Child Support Enforcement, and Medical Services).
15. Business Continuity - A proactive process identifying the key functions of an organization and the likely threats to those functions. From this information, plans and procedures can be developed which ensure key functions can continue whatever the circumstances.
16. Bureau/Office Web Administrator - This position is designated by the Bureau Commissioners or Office Directors. Within their respective Bureaus or Offices, this person is responsible for coordinating with the DHHR Web Administrator concerning the Bureau/Office Web site and maintaining the site to provide timely and up-to-date information.
17. Central Facility Management (CFM) - Responsible for the governing of policies and procedures for the Diamond Building.
18. Central Processing Unit (CPU) - The part of a computer that interprets and executes instructions.
19. Chief Technology Officer (CTO) - The director of MIS and the person responsible for all information resources within the DHHR.
20. Computer Virus - Software used to infect a computer with a destructive program.
21. Computing Resources - computer hardware, servers, PC's, workstations, terminals, printers, and other equipment physically located within the DHHR.
22. Confidential Information - All information not in the public domain.
23. Configuration Files - These files contain special commands, which set up the computer's hardware components and load the device drivers (e.g., memory, mouse, printer) so the applications can use them.
24. Control - a protective action, device, policy, procedure, technique, or other measure that reduces exposure.
25. Critical Business Data - Data that must be backed up frequently because of its importance to the IT system.
26. Cryptography - The process or skill of communicating in or deciphering coded information.
27. Custodian of an Information Resource - the unit assigned to supply services associated with particular data.
28. Data/Resource Owner - The person having primary responsibility for the creation and maintenance of the data content.
29. Data Center Desktop Support (DCDS) - The OMIS organization that is responsible for the DHHR Data Center as well as all Kanawha County offices.

30. Database - An organized collection of information that can be searched, retrieved, changed, and sorted using a collection of programs known as a database management system.
31. Database Administrator (DBA) – A person with a high degree of technical expertise who is responsible for the design and management of an organization's database.
32. Decryption – The process of unscrambling data using a password or key, so that it is unintelligible. Decryption is the only necessary when a file has undergone encryption.
33. Degauss - To demagnetize data from storage devices in order to destroy the media so it is no longer usable.
34. Demilitarized Zone (DMZ) – A network added between a protected network and an external network in order to provide an additional layer of security. (sometimes called a perimeter network.)
35. Destruction to Information Assets – Deliberate, or through negligence, damage to or destruction of manual or computerized information, computer programs, computer hardware, computer peripherals such as printers, or computer networks.
36. Device – Including but not limited to personal computers, laptops, handheld units (PDA's).
37. DHHR Office of Personnel Services – A division that reports directly to the Assistant Secretary for Operations and has three main units. They are: Employee Information, Third Level Grievance Evaluator, and Special Projects. This office is generally responsible for the Department-wide personnel activities and interaction with the WV Division of Personnel.
38. DHHR HIPAA Privacy Officer – Individual designated by the DHHR, who is responsible for the development and implementation of privacy policies and procedures for the purposes of HIPAA privacy regulations.
39. DHHR Secretary – This position is appointed by the Governor. With the advice and consent of the Senate, this individual is the administrative head of the Department. The Secretary serves at the will and pleasure of the Governor for the term of which the Governor is elected and until a successor has been appointed and has qualified.
40. DHHR HIPAA Security Officer - Individual designated by the DHHR, who is responsible for the development and implementation of security policies and procedures for the purposes of HIPAA security regulations.
41. DHHR Web Administrator – This position is appointed by the CTO and manages the content of the DHHR's Internet and Intranet. The Web Administrator determines the administrative needs and requirements for the DHHR web presence and works with the OMIS NTS group to carry out and enhance the technical aspects of operating the network server.
42. Disaster - Any event that makes an organization unable to provide critical business functions for a pre-determined period of time. This may include: any occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property resulting from a natural, technological, and/or national security incident, (ex: fire, vandalism, natural disaster, or system failure).

43. Disaster Recovery Coordinator - The person responsible for ensuring that all Bureaus and Offices within DHHR have a plan for restoration of information and operations following a disaster.
44. Disaster Recovery Plan – A plan that applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. This IT focused plan is designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.
45. Disposal - The final disposition of electronic data, and/or the hardware on which electronic data is stored.
46. Electronic Protected Health Information (e-PHI) – Health information transmitted by or maintained in electronic media used to identify an individual, which is created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.
47. E-mail – Any message sent electronically through one or more computers and/or communications networks, and in most cases has a human originator and receiver.
48. E-mail System – A service that sends messages on computers via local or global networks. E-mail systems provide for storage, and later retrieval of messages and attachments, as well as real-time communication.
49. Emerging Technologies – Technologies that are yet to be invented or implemented within the DHHR.
50. Employee - Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractors' employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.
51. Encryption – The process of enciphering or encoding data so that it is inaccessible to unauthorized users.
52. Equipment Coordinator (EC) – Designated employees in DHHR field offices, Child Care Resource and Referral agencies, and Local Health Departments who are responsible for providing first level computer support. ECs receive computer support direction from OMIS.
53. Falsification of Information – Unauthorized alteration of computerized information, computer programs, or information in any other form. The alteration can be for any reason, including: fraud, embezzlement, personal gain, or aiding in the perpetration of a crime.
54. File Transfer Protocol (FTP) - The TCP/IP protocol enabling users to copy files between systems and perform file management functions, such as renaming or deleting files.
55. Firewall – A network node set up as a boundary to prevent traffic from one segment to cross over to another. Firewalls are used to improve network traffic, as well as for security purposes.

56. Flex Time – An alternative schedule used by permanent, full time employees which varies their work routine from normal business hours (eight hours a day, Monday through Friday), yet still gives them a 40-hour work week.
57. Flex Time Cycle – The flex time cycle consists of three month periods and begins and ends on the nearest full week. Once an employee starts the program, the schedule is in effect until the end of the existing three month period.
58. General Counsel – The legal unit of the DHHR that provides timely and accurate legal advice and counsel to the Secretary and the Department. The General Counsel enhances the DHHR's decision-making process by providing effective legal advice.
59. Hardware - A computer, its components, its peripherals, and other associated equipment - any physical object that is part of a computer system.
60. Home Page – This is a starting point for DHHR Bureaus/Offices to place links to other parts of the Web. For example, the DHHR home page is not lonely linked to all DHHR Bureaus and Offices, it is also linked to the main State of West Virginia Home page, various county health departments, federal agencies, and other health related web pages.
61. Incident – An adverse event associated with an information system that: (1) fails to comply with security regulations or directives; (2) results in attempted or actual loss of data; (3) involves the waste, fraud, abuse, loss, or damage of property or information; and (4) reveals and/or exploits hardware or software vulnerabilities.
62. Information Resources – A collection of manual and automated components, each managing a specific data set or information resource.
63. Information Security Incident – An event involving (1) unauthorized modification, distribution, or destruction of automated or manual information; (2) unauthorized disclosure of or access to automated or manual information; or (3) loss of, damage to, or misuse of information assets.
64. Information Security Officer (ISO) - The person designated by the CIO to monitor and provide initial enforcement of DHHR's information security program and IT policies.
65. Integrity – The ability for an entity to protect data from improper alteration or destruction and to assure e-PHI in its possession is kept consistent with its source.
66. Interoperability – the ability of a system to use the parts or equipment of another system.
67. IT Assets – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.
68. IT Policies – Written statements defining requirements and compliance mandates in the conduct of Departmental IT affairs to Bureau Commissioners and other members of the DHHR community. Only the Secretary, as chief administrative officer of the DHHR, may issue policy statements, including those relating to IT.
69. Jump Drive – A small self-powered drive that connects to a computer directly through a USB port.

70. Key – A character string used to encrypt data. The key must be known in order to decrypt the data.
71. Key Pad Unit – A security unit located outside the computer room which allows authorized personnel to key in a numbered code to gain entry.
72. LAN – A communications network made up of servers, workstations, a network operating system, and a communications link that serves users within a confined geographical area.
73. Magnetic Media - Any type of mass storage that holds information magnetically.
74. Malicious Code – Computer instructions, usually in the form of a program, designed to perform undesired changes to the computer system, data, or programs. (Ex: computer virus)
75. Mass Mailings – Information shared with a group of people who all need to know the same material, (ex., committee members, individual units within Bureaus, etc.).
76. Media Controls - Formal, documented, policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.
77. Mission Critical Information – information that is defined by the DHHR to be critical to the DHHR's function(s).
78. Misuse of Information Assets – This occurs when information is read, copied or used for purposes that are not authorized or when information resources are used for unauthorized purposes.
79. Network – A system of computers, and often peripherals, such as printers, linked together. DHHR workstations are connected to a Wide Area Network (WAN), which is a larger network, which uses telephone lines or radio waves to link computers that can be up to thousands of miles apart.
80. Network Monitoring – Detection of break-ins or break-in attempts by reviewing logs or other information available on a network. Intrusion detection is essential for maintaining network security.
81. Network Monitoring Tools – Automated software tools that perform real-time analysis of data traffic, and employ advanced logic to detect patterns of activity that indicate that an intrusion attack is underway.
82. Network Personnel – Those personnel who have constant access to the computer room and are needed to operate and/or maintain the equipment.
83. Network Security – Measures taken to protect a communications pathway from unauthorized access to, and accidental or willful interference of, regular operations.
84. Network Security Database – This will be established and maintained by the CIO. The purpose of the database is to maintain up-to-date contact information that will identify the emergency contact during a computer or network security incident, and for the dissemination of guidelines and procedures for network security.

85. Network and Technical Support (NTS) – The OMIS organization responsible for engineering and emerging technologies, Help Desk/Customer Support, and field support.
86. Non-Network Personnel – Those personnel who do not need access to the computer room on a daily basis. These individuals must have prior approval and submit a written request of their needs for computer room access.
87. Non-Records – Messages consisting of informational records created primarily for the informal communication of information. These messages are short-lived, and do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt.
88. Notification/Activation Phase – The process of notifying recovery personnel and performing a damage assessment following a system disruption.
89. Office of the Inspector General (OIG) - The office designated by the DHHR Secretary to investigate and/or assist in investigating allegations of employee abuses or misconduct.
90. Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.
91. OMIS Help Desk – The first level of support for network users. Help Desk support includes problem resolution, call escalation, vendor support, and customer relations.
92. OMIS Managers - Senior IT professionals who report directly to the CTO and perform advanced level administrative and supervisory duties. These managers have oversight of several units of technical and supervisory staff such as: programming, support services (including LAN management), networks support, and/or data center management. They also provide leadership in the planning and implementation of DHHR-wide IT needs.
93. On call – Employees may be placed “on call” during any day of the week. During this time, they can be contacted by phone or beeper and must be available to come to work if special circumstances dictate this course of action.
94. Operating Procedure – A series of steps followed in a definite regular order ensuring the consistent and repetitive approach to actions.
95. Operating System - System software that controls the way different pieces of hardware operate, and the way the computer responds to commands.
96. Operations Unit – A unit reporting directly to the DHHR Deputy Secretary for Administration that is charged with providing management and policy training to all DHHR personnel.
97. Oracle System – A database management system developed by Oracle Corporation that runs on Unix and Microsoft Windows.
98. PC – A personal computer; also called a workstation.

99. Personal Identification Number (PIN) - A number or code assigned to an individual and used to provide verification of identity.
100. Physical Security – refers to the protection of building sites and equipment (and all other information and software contained within) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage.
101. Portable Computers – Computers which are easily moved from one location to another. This includes laptops, notebooks, tablet PCs, PDAs, and Smartphones.
102. Priority One – The highest level of action priority assigned to a technician by the OMIS Help Desk. This priority level is used when the largest number of users is affected and corrective action must be taken immediately.
103. Privacy Officer – This person is responsible for creating, obtaining management approval, implementing, and maintaining a comprehensive contingency plan.
104. Public Key Encryption – The encryption of data using two different keys - public and private – for encryption and decryption. Public key encryption is useful in situations in which a sender and recipient wish to communicate securely and in which speed is not important.
105. Reconstitution Phase – This phase outlines actions that can be taken to return the system to normal operating conditions following a system disruption.
106. Records – Documentary materials or information, regardless of physical media or characteristics, made or received by an office in connection with the transaction of official business and preserved by that office as evidence of the DHHR’s functions, policies, decisions, procedures, operations, or other activities of that office, or because of the value of the data in the record.
107. Recovery Phase – This phase discusses a suggested course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities following a system disruption.
108. Reference PC - A PC on which new packages for software distribution are created. It runs the SWD Assistant to compile the software changes made into a package.
109. Retention – Specifies how long the e-mail (sent or received) needs to be kept to satisfy administrative, legal, fiscal, and historical requirements.
110. Risk Analysis – A process where relevant assets and threats are identified, and cost-effective security/control measures are identified or engineered to effectively balance the costs of various security/risk mitigation/control measures against the losses that would be expected if these measures were not in place.
111. Risk Assessment – An evaluation of the following: (1) the exposure of an asset to the identified threats; (2) the potential impacts of an event; (3) an estimate of the likelihood of an event occurring; and (4) the effectiveness of existing or proposed safeguards to protect an asset.
112. Risk Management – The process of analyzing exposure to risk and determining how to best handle such exposure.

113. Sanitization - The process of rendering data harmless.
114. Scan – To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors, et. al.).
115. Secure Sockets Layer (SSL) – An encryption standard used to transmit data securely over the Internet.
116. Security Breach – an event resulting in unauthorized access, loss, disclosure, modification, or destruction of information resources, whether accidental or deliberate.
117. Sensitive Information – Information/data that would be disadvantageous should it become known to others (ex: political/religious beliefs, health information, or criminal record).
118. Server - A shared computer that supports the processing, communications, or file management of other computers on a network.
119. Server Room – secure room that houses a computer or processor holding applications, files, or memory shared by users on a network.
120. Shareware – Copyrighted programs made available on a trial basis.
121. Snapshots - An image of the state of the system taken by the SWD Assistant and kept for later reference. The snapshot contains information about all files and directories on the reference PC together with information on all Program Manager groups and icons. It is used by the SWD Assistant to determine the changes which took place when a particular software product was installed on the reference PC.
122. Software – The programs, programming languages, and data that control the functioning of the hardware and direct its operations. It is usually divided into two categories: systems software and applications.
123. Software Depot - A file server that stores the software packages which can then be retrieved by the target PC's when needed.
124. Software Distribution (SWD) Assistant - Creates ready to distribute packages by memorizing the configuration of a system before and installation, and then uses it to find the changes that took place after the installation.
125. Software Distribution Package - This package contains the instructions and files necessary to install an application. It consists of a single compressed archive, which includes the created files and a script for the installation.
126. Software license – A legal agreement between the developer and the user of software that specifies the conditions for distributing, storing, and using that software.
127. Software upgrade – To replace a software program with a more recently released version.

128. Streaming Audio/Video - The sending and displaying of audio or video in real time over the Internet, instead of first sending a file and displaying it after it has been downloaded.
129. Structured Query Language (SQL) - A standard interface language for the issuing of queries to a relational database.
130. Target PC - The PC to which the software package is to be distributed.
131. TCP/IP - Two interrelated protocols for network communications routing and data transfer. TCP is used to break data into packets, and IP routes the packets.
132. Testing and Revision - A documented process of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation if necessary.
133. Unauthorized Access - Access by a person whose job duties do not require specified access to a computer or computer system.
134. Unauthorized Disclosure - Release of any information to a person who is not authorized to receive it. (Ex: Disclosure of a password)
135. USB Port - A device used for connecting peripherals (printer, scanner, modem, etc.) to a PC off of a single port.
136. User - Any individual who creates content to be placed on DHHR web servers.
137. User of an Information Resource - the person who has been granted explicit authorization to access the data by the owners.
138. Virtual Private Network (VPN) - A way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.
139. Virus Detection Software - Software that defends a PC against viruses and other malicious Internet code by scanning incoming attachments in e-mail and from other programs.
140. Web Page - A single page displayed by a Web browser.
141. Web Server - A server on the Internet that holds World Wide Web documents and makes them available for viewing by remote browsers.
142. Wide Area Network (WAN) - A communications network connecting computing devices over geographically distant locations. A WAN covers a much larger area than a LAN, such as a city, state, or country. WANs can either use phone lines or dedicated communication lines.
143. Workstation - an electronic computing device (i.e., laptop or desktop computer), or any other device that performs similar functions, and the electronic media stored in its immediate environment.