ODH Directive 7B
USE AND SECURITY OF AGENCY IT RESOURCES

Encl:
(1) Information Technology Code of Responsibility, HEA 6200
(2) Request for Academic Use of ODH Computer Resource, HEA 0302

Reference:
(1) ODH Directive 24, Data Stewardship
(2) ODH Directive 26 - Safeguarding Assigned ODH Equipment
(3) Ohio IT Policy ITP-A.26, Software Copyright Compliance
(4) Ohio IT Policy ITP-B.1, Information Security Framework
(5) Ohio IT Policy ITP-B.2, Boundary Security
(6) Ohio IT Policy ITP-B.3, Password and Personal Identification Number Security
(7) Ohio IT Policy ITP-B.4, Malicious Code Security
(8) Ohio IT Policy ITP-B.5, Remote Access Security
(9) Ohio IT Policy ITP-B.6, Internet Security
(10) Ohio IT Policy ITP-B.7, Security Incident Response
(11) Ohio IT Policy ITP-B.8, Security Education and Awareness
(12) Ohio IT Policy ITP-B.9, Portable Computing Security
(13) Ohio IT Policy ITP-B.10 Security Notifications
(14) Ohio IT Policy ITP-B.11 Data Classification
(15) Ohio IT Policy ITP-B.12 Intrusion Prevention and Detection
(16) Ohio IT Policy ITP-E.1, Disposal, Servicing and Transfer of IT Equipment
(17) Ohio IT Policy ITP-E.7, Business Resumption Planning
(18) Ohio IT Policy ITP-E.8, Use of Internet, E-mail and Other IT Resources
(19) Ohio IT Policy ITP-E.30, Electronic Records
(20) Ohio IT Policy ITP-F.1, Registration of Internet Domain Names
(21) Ohio IT Policy ITP-F.3, Web Site Accessibility
(22) Ohio IT Policy ITP-F.4, Web Site Standardization
(23) Ohio IT Policy ITP-F.35, Moratorium on the Use of Advertisements, Endorsements, And Sponsorships on State-Controlled Web sites
(24) Ohio IT Policy ITP-H.2, Use of State Telephones
(25) Ohio IT Policy ITP-H.6, Telecommunications Utility Services
(26) OMIS Letter 1, Backup Tape Rotation
(27) ITS-SEC-01, Data Encryption and Cryptography

1. **Purpose.** The purpose of this policy is to provide Ohio Department of Health (ODH) staff with guidelines regarding the use and the security of the all agency IT resources such as Internet Use, E-Mail Use, and the use of the agency's information and data resources. This directive supersedes any past practice, previously issued directive, or previously issued policy, and will remain in effect until canceled or superseded. The Office of Management Information Systems (OMIS) is responsible for the drafting of this Directive. The agency Network Manager shall serve as the Data Privacy Point of Contact

(DPPOC) for OIT and for the agency security systems and shall annually certify that all program requirements are met.

2. Introduction. While ODH recognizes that data access offers an effective means for making government agencies more accessible, efficient, and responsive to the needs of other government agencies and the public, its availability is open to misuse. This policy establishes controls on the use of state-provided and authorized information technology (IT) resources to ensure they are appropriately used for the purposes for which they were acquired or approved.

2.1. Opportunities and Risks. ODH furnishes or authorizes a variety of IT resources to conduct the business of the state. These resources include desktop and notebook computers, tablet PCs, printers, digital copiers, portable storage devices, personal digital assistants, digital audio and video recorders; software, subscription services, e-mail and Internet; and supplies such as paper, toner, and ink. Restrictions on the use of ODH IT resources outlined in this policy also apply to wired as well as wireless telephone devices and services, including, but not limited to, facsimile machines connected to the state's telephone service.

With such a proliferation of devices, services and software, great care is required to prevent misappropriation of publicly owned IT resources and data. The wide array of resources, services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to these opportunities and risks, this directive describes ODH's official policy regarding Use and Security of the Agency IT Resources.

2.2. Applicability. This policy applies to all staff at ODH using ODH resources (e.g. employees, contractors, temporary workers, students, student interns, volunteers, and other agents of the state who use and administer ODH resources). All ODH staff are expected to be familiar with and comply with this policy. Questions about the policy should be directed to ODH staff supervisors and project managers.

A violation of the provisions of this directive may be grounds for adverse administrative (including revocation of system privileges) and/or disciplinary action up to and including removal.

In addition to this ODH policy, collective bargaining contract provisions provide guidance on the use of state-provided IT resources for contract enforcement, interpretation, and grievance processing.

2.3. Acknowledgement. All ODH staff shall read and sign the form, Information Technology Code of Responsibility, Enclosure (1), attached hereto. The signed copy shall be filed in each employee's personnel file. The Office of Human Resources shall ensure that new employees complete Enclosure (1) at the time of orientation. If access is required by contractor personnel, temporary workers, or others who do not attend orientation, the responsible ODH staff supervisors and project managers must obtain a signed copy before the start of work and annually thereafter.

3. Data Confidentiality. ODH is responsible for protecting and promoting the health of Ohioans. Therefore, many ODH programs routinely receive and maintain personal information including personal health-related information and vital records (e.g. original birth, death, fetal death records and abstracts of marriage and divorce). Maintaining the confidentiality of personal information, when appropriate, and the public trust is imperative for ODH to accomplish its mission. ODH staff must be aware of their responsibility to comply with all applicable state and federal confidentiality statutes, rules, regulations, as well as state, departmental, and programmatic policies. Any non-authorized data access and/or disclosure is strictly prohibited.

3.1. When state and federal law establishes that personal information is confidential, copying or transmitting such personal information in an unauthorized manner is prohibited. The information which resides on these documents can be used to propagate false documentation and facilitate fraud and identity theft. Any violation of this policy or unauthorized copying or transmittal shall be deemed a breach of confidentiality according to applicable state and federal law.

3.2. Any personal information that is not public record must not be shared or allowed to be viewed by anyone at ODH, any other agency or other persons unless authorized by Ohio law or written departmental or program policy or by the ODH staff supervisors and project managers..

3.3. In the course of working at ODH, staff may inadvertently receive confidential information which is not part of their normal job duties; if this happens, staff shall discreetly give this information to their ODH staff supervisors and project managers, discretely give the confidential information to the correct program area or confidentially return the information to the sender.

3.4. Many programs that routinely collect personal information have specific laws and rules that indicate who may have access to these data; furthermore, if these programs have additional procedures for ODH program staff for protecting confidential information, these procedures will be supplied to the staff by their supervisors and project managers . All information specifically about ODH employees as part of their public sector employment is addressed specifically in Ohio law and not covered by this policy.

4. Information Integrity.

4.1. Information Reliability. The accuracy / veracity of all information taken from the Internet should be considered suspect until confirmed. There is no quality control process on the Internet. Information on the Internet may be outdated, inaccurate, and in some instances, misleading.

4.2. Downloading Software. The computers used at ODH are part of a complex network and the software on each computer can affect this network. All software to be installed on a computer, including software downloaded from the Internet, must be approved as outlined in the OMIS Standard Operating Procedures (SOP) documentation. This may include authorization of individual software programs as well as an agency-wide authorization for specific products (e.g., the freeware version of Adobe Acrobat). Updating

of software or information on ODH computers via technology that automatically updates software on a personal computer, server, or other network attached device via a connection to the Internet ("push technology") is prohibited unless the involved system has first been tested and approved by the Chief of OMIS, the Network Manager or a designee.

4.3. User Anonymity. Misrepresenting, obscuring, suppressing, or replacing a user's identify on the Internet or any ODH electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. If users have a need to employ re-mailers or other anonymous facilities, they must do so on their own time, with their own information systems, and with their own Internet access accounts. Staff should only access the Internet using his or her own ODH network account.

4.4. Web Page Updates. ODH staff must follow the established Internet Web Sites Guidelines for posting information. Instructions can be found on the ODHNet, under Policies/Forms "W" Web (Internet and Intranet / ODHNet sites) for modifications including the addition of hyperlinks to other sites, updating the information displayed, and altering the graphic layout of a page. All Internet Web Sites shall comply with Ohio IT Policies ITP-F.1 (Registration of Internet Domain Names), ITP-F.3 (Web Site Accessibility), ITP-F.35 (Moratorium on the Use of Advertisements, Endorsements, And Sponsorships on State-Controlled Web sites) and the ODH Web Addresses policies.

5. Information Confidentiality.

5.1. Encryption. Message interceptions are not technically difficult and are frequently encountered on the Internet. Accordingly, ODH confidential information must not be sent over the Internet unless it has first been encrypted by approved methods.

5.1.1. Only approved OMIS encryption methods and procedures shall be used.

5.1.2. ODH staff shall only encrypt information as approved or directed by a manager and OMIS. ODH managers will follow the minimum encryption standards identified in Ohio IT Standards ITS-SEC-01 (Data Encryption and Cryptography). This State IT standard defines the minimum requirements for cryptographic algorithms that are cryptographically strong and are used in security services that protect at-risk or non-public data as defined and required by agency or state bulletin, policy or rule.

5.1.3. Uncontrolled and unauthorized use of non-public information on privately owned devices (e.g. cell phones, portable memory devices, messaging or texting devices, cameras) of ODH staff is prohibited.

5.1.4. Unless information is specifically designated to be public information by staff managers, data must always be encrypted before being sent over the Internet or transported outside of ODH.

6. Portable Computing Security. Unless otherwise specified in Agency specific or OMIS policies, OMIS procedures for Portable Computer Security shall comply with the

Ohio IT Policy ITP-B.9 (Portable Computing Security). ODH Directive 26 (Safeguarding Assigned ODH Equipment) contains a list of additional safeguards that supplement the Ohio IT Policy ITP-B.9 (Portable Computing Security). ODH staff shall comply with the above referenced policies and procedures and ODH Directive 26.

6.1. Individually Identifying Information. Following applicable state and federal laws, as well as, departmental and program policies, ODH staff must be aware of their responsibility to prevent breaches involving the data containing the public's personal identifying information. ODH staff must practice sufficient security protection as defined in Ohio IT Policy ITP-B.3 (Password and Personal Identification Number Security), Ohio IT Policy ITP-B.9 (Portable Computing Security) and ODH Directive 26 (Safeguarding Assigned ODH Equipment) when using mobile devices and data storage media (e.g., notebook computers, tablets, external USB drives, PDAs, data CDs and DVDs, and USB flash drives) including the use of encryption for data files containing non-public information.

6.2. Operation and Maintenance.

6.2.1. Mandatory system configurations, settings and software for either state-owned or authorized non-state owned devices shall be maintained and shall not be modified without prior authorization by designated ODH personnel or using ODH procedures. Device operating systems shall be maintained with the approval of ODH OMIS using appropriate vendor security patches and updates. ODH employs various firewall technologies, inbound E-Mail protection, workstation spyware protection and enterprise virus protection in accordance with Ohio IT Policy ITP-B.12 (Intrusion Protection and Detection). Devices shall be equipped with anti-virus software and firewalls in accordance with ODH procedures. Devices are subject to inspection by OMIS staff to ensure compliance. Compliance confirmation is required for direct access to the agency network.

6.2.2. A PC is safest when it is turned off. ODH staff shall turn off PCs when they will not be used for an extended period, such as at night or while in class. Turning off a PC can greatly decrease a PC's chance of contracting a virus.

6.2.3. Device configurations shall comply with the minimum ODH computing requirements. State-owned portable computing devices shall be returned to the manager when the user's employment or contract terminates, or the user's assignment no longer requires the state-owned device. No ODH user shall place non-state data and software on state-owned devices. When a device is removed from service, ODH shall sanitize the IT equipment to remove information.

6.2.4. In order to ensure the accountability and safeguarding of ODH assets, all ODH employees shall follow the procedures outlined in ODH Directive 26A (Information Technology & Sensitive Equipment Management) regarding the receipt, distribution, inventory and storage of ODH Information Technology and Sensitive Equipment.

6.2.5. Staff shall maintain a copy of state data on the ODH network, which OMIS performs regular system and data back-ups as frequently as needed based on the risk assessment of the information maintained on the portable device. Back-ups shall be safeguarded and retained for a period commensurate with the value and criticality of the

information. Backups will be accomplished in accordance with OMIS Letter 1 (ODH Backup Tape Rotation) which contains detailed information on timing and procedures related to data backup and storage.

6.2.6. All state data and software will be recovered, deleted and securely overwritten as appropriate from state-owned, privately owned and contractor-owned computing devices when the user's employment or contract terminates or when the computing device is no longer authorized for official state business. ODH is not liable for the loss of non-state data or the confidentially of data synced to state-owned or approved operated devices. Written approval must be obtained before the privately owned or contractor-owned devices may be used for official state use.

6.2.7. ODH staff shall follow OMIS procedures for loaning, donating, servicing, or disposing of IT equipment which comply with the Ohio IT Policy ITP-E.1 (Disposal, Servicing, and Transfer of IT Equipment).

6.2.8. IT property, which contains batteries, shall be disposed in accordance with Ohio Administrative Code Chapter 3745-273 and the federal Mercury-Containing and Rechargeable Battery Management Act (42 USC Sec.14301 et seq., 1996). All other applicable state and federal mandates regarding disposal of state IT property containing hazardous materials shall be followed.

6.3. Business Continuity. In accordance with Ohio IT Policy ITP-E.7 (Business Resumption Planning), OMIS and ODH data stewards shall maintain a business resumption plan for computer and communications services. The business resumption plan shall include scenarios for fire, natural disaster, extended power loss, civil disorder, or bomb threats.

7. System Security. In accordance with Ohio IT Policy ITP-B.1 (Information Security Framework), Ohio IT Policy ITP-B.2 (Boundary Security), Ohio IT Policy ITP-B.5 (Remote Access Policy) and ODH Directive 24 (Data Stewardship), ODH staff shall follow procedures regarding access privileges, authentication methods, risk management, system hardening, network monitoring, audit logging, breach monitoring and communications/notification methods to comply with applicable laws, regulations, policies, guidelines, and standards.

7.1. Telephones and Telecommunications. ODH employees are assigned state owned cellular telephones and wired telephones (traditional landline, local and long distance telephone service) in order to facilitate communication in the course of performing state business. Any telephones issued are the property of ODH. In accordance with Ohio IT Policy ITP-H.2 (Use of State Telephones) and Ohio IT Policy ITP-H.6 (Telecommunications Utility Services), ODH staff shall follow procedures regarding access, approval, privileges, and operations to comply with applicable laws, regulations, policies, guidelines, and standards.

7.1.1. Personal Telephone Usage. The Director of Health recognizes that it may be necessary to make or accept a limited number of local personal telephone calls while at work. However, the frequency and duration of such calls must be kept to a minimum and,

whenever possible, made during lunch or authorized breaks. Personal business, which involves an activity undertaken for profit or gain of any kind, shall not be conducted from a state telephone. Employees are prohibited from circulating their state telephone number as a telephone number at which they can be reached for personal business (personal business cards and materials shall not have a state telephone number listed as the contact number). Except in the case of emergencies, personal long distance calls shall not be made from wired telephones and charged to the state. Personal long distance calls can be made from wired state telephones if charged to a personal credit card, to a third party number or a non-state number. ODH may exclude some state telephones from receiving or originating any personal calls. Calls to 1-900 numbers or other pay-per-call numbers are strictly prohibited.

7.1.2. Cellular Telephones. In addition to traditional wired telephones, state employees are increasingly using cellular telephones. Usage costs for cellular service are higher than wired telephone service, and cellular service is subject to a higher risk of fraud. Hence, there is a higher fiduciary responsibility to oversee and regulate cellular telephone use and payment of invoices. A written work order, approved by the Program's Divisional Administration Office Chief, to the ODH Telecommunications Coordinator is required to issue a cellular telephone.

7.2. Electronic Signatures. ODH staff shall follow electronic Signature procedures which comply with Ohio Administrative Code section 123:3-1-01 and Ohio IT Policy ITP-B.3 (Password and Personal Identification Number Security).

7.3. Records Management. Electronic records are subject to audit and legal proceedings. Records management procedures shall comply with Ohio Revised Code chapters 149 and 1306, Ohio IT Policy ITP E.30 (Electronic Records), American National Standards Institute or other industry-wide standards, Office of Statewide IT Policy (ITP)-issued best practices and/or Electronic Records Committee (ERC)-issued guidelines. ODH staff shall follow procedures which employ best practices from open, public, non-proprietary standards that facilitate communication between multiple systems and software.

7.4. Data Classification. Data shall be appropriately classified, and related management controls shall be in place in accordance with Ohio IT Policy ITP-B.11 (Data Classification) and ODH Directive 24 (Data Stewardship).

7.5. Confirmation of User Access Listing (COAL). ODH staff supervisors shall complete an initial and yearly review of each user's network and information / data access rights. The initial and annual review, documentation and affirmation of each employee's network and data access rights will be performed as follows:

- OMIS will create the Employee Performance Evaluation (EPE) quarterly schedule listing that includes a personnel listing, and their supervisor of the rating period, one quarter in advance
- OMIS will perform a complete user access rights review for each employee, using the EPE quarterly schedule, to include:
    - File System Access (e.g. Home Area, Shared Areas, etc.)

  - Database Access
  - Application Access
- OMIS will create a COAL document for each employee
- OMIS will provide the COAL document to the employee's supervisor, per the EPE schedule, for use during each employee's EPE
- The supervisor will review the employee's COAL document with the employee as part of the annual EPE. If modifications are necessary, the supervisor will document them on the COAL document during the EPE
- The supervisor and the employee will sign the COAL document after completing the review and forward it to OMIS for verification
- If modifications were made to the COAL document, OMIS will make the requested modifications per the returned COAL document
- At the end of each EPE quarter, OMIS will perform a verification to insure all supervisors have provided a signed copy, paper or electronic, of each employee's COAL within 2 weeks after the end of the EPE quarter.
- In the event a COAL is not provided for an employee, OMIS will attempt to contact the supervisor of the employee to attempt to acquire the employee's delinquent COAL document. In the event that a COAL remains delinquent, OMIS will immediately disable the employee's network, application and data access until such time that the employee's supervisor provides a copy of the signed COAL

7.6. Information Technology Code of Responsibility (ITCOR). A yearly review and acknowledgement of ODH's Information Technology Code of Responsibility will be performed by all ODH staff as part of the annual Employee Performance Evaluation using HEA 6200 Information Technology Code of Responsibility.

8. Public Representation.

8.1. External Representations. Any use of state-provided IT resources to operate, participate in, or contribute to an online community including, but not limited to, online forums, chat rooms, instant messaging, listservs, blogs, wikis, peer-to-peer file sharing, and social networks, is strictly prohibited unless organized or approved by the agency. If an individual is approved to participate in any of these forms of communication as part of state business, that individual shall at all times, act professionally and shall fulfill agency-defined security education and awareness requirements for proper use before participating. The content of the education and awareness requirements shall include methods to avoid inadvertent disclosure of non-public information and practices to avoid that could harm the security of state computer systems and networks.

8.2. Removal of Postings. Messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, which include an implied or explicit affiliation with ODH, may be removed if ODH management deems them inconsistent with ODH's interests or existing policy. When practical and feasible, individuals responsible for the message will be informed of the decision and given the opportunity to remove the message(s) themselves.

9. Appropriate Behavior. Professionalism and courtesy not only enhances the public image of the Department but also minimizes the possibility of legal issues associated with libel and defamation of character. Therefore, ODH staff shall, at all times when using agency IT resources, be professional and courteous. "Flaming" or similar written attacks are strictly prohibited. All messages that might be perceived to threaten, harass, annoy, or alarm another person or organizations are also strictly prohibited.

10. Disclosure of Information. Care must be taken to properly structure comments and questions posted to automated mailing lists (listservs), public news groups, and related public postings on the Internet. Before posting any material, ODH staff must consider whether the material could potentially disclose confidential information or embarrass ODH or the state. Consulting the Office of Public Affairs or the Office of the General Counsel is advised if staff have questions. ODH staff shall take all reasonable precautions to prevent the inadvertent dissemination of non-public information via the Internet.

11. Software Licensing and Intellectual Property Rights. ODH shall employ proper acquisition, inventory, installation, storage, disposal and auditing of software in accordance with Ohio IT Policy ITP-A.26 (Software Licensing) and Ohio IT Policy ITP-E.8 (Use of Internet, E-Mail and Other IT Resources). ODH and ODH staff shall also support licensing agreements that maintain the ownership rights of intellectual property holders while also following all federal copyright laws. ODH staff will educate themselves on software licensing policies by participating in periodic ODH-prepared user awareness training.

12. Access Control.

12.1. Internet Service Providers. ODH staff must not employ Internet Service Provider (ISP) accounts and dial-up lines to access the Internet with ODH computers without prior approval from the Chief of OMIS or designee. This includes using third parties to host listservs.

12.2. Establishing Network Connections. Unless the prior written approval of the Chief of OMIS has been obtained, ODH staff may not establish Internet or other external network connections that could allow non-ODH users to gain access to ODH systems and information. These connections include the establishment of modem dial-up, electronic data interchange (EDI), Internet web pages, FTP servers, and the like.

Installing, attaching or connecting (physically or wirelessly) to any ODH IT resource, without prior authorization, is strictly prohibited. Connecting or attempting to connect a wireless device to the state's wireless service without proper agency approval is strictly prohibited.

13. Business and Personal Use.

13.1. Personal Use. Access to and the security of the all agency IT resources are to be used by ODH staff primarily for ODH business purposes. However, personal use of the Internet is permitted on personal time. Use of ODH computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible,

so long as no ODH business activity is preempted by the personal use and so long as users follow Ohio IT Policy ITP-B.6 (Internet Security). Uses that interfere with normal ODH business activities, involve solicitation, are associated with any for profit business activities, or which could potentially embarrass ODH or the state are strictly forbidden. ODH staff must not employ the Internet or ODH information systems in such a way that the productivity of other staff is eroded (examples include chain letters, broadcast charitable solicitations, and lengthy exchanges between employees on non-business matters). ODH computing resources, including printers, may be used for academic or training courses during non-work hours (e.g., before and after scheduled workdays and on weekends). Such courses must serve to enhance those skills or abilities related to the employee's current or potential employment at ODH. The employee is responsible for providing his or her own paper if a printer is to be used. The form, Request for Academic Use of ODH Computer Resource, Enclosure (2) attached hereto, must be completed and approved prior to any non-work hours use of ODH computer resources.

13.2. Prohibited Uses. ODH staff shall not use the Internet or the agency IT resources for operating a business for personal gain, non-work audio programs such as radio stations, sending chain letters, gambling or wagering, accessing personal services (e.g., dating services), or soliciting money for religious and political causes. ODH staff are prohibited from circulating their state e-mail address or phone numbers as a means at which they can be reached for personal business (personal business cards and other personal business materials must not have a state e-mail address listed). ODH staff shall not use the Internet to transmit or download material that is defamatory, racially or sexually harassing, threatening, obscene, pornographic, or which may contribute to a hostile work environment. Among other things, a hostile work environment is created when derogatory comments about a certain sex, race, religion, or sexual orientation are circulated. ODH staff shall not use the Internet to transmit or download material that would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability. ODH staff shall not use the Internet to disseminate or print copyrighted material (including articles and software) in violation of copyright laws. ODH staff shall not use the Internet to provide access to confidential information. Violating or supporting and encouraging the violation of local, state or federal law is strictly prohibited. These prohibitions apply to business and personal use as defined above.

14. Privacy Expectations.

14.1. No Default Protection. ODH staff using the Internet or other agency IT resources should realize that their communications may not be protected from viewing by third parties.

14.2. Logging. ODH staff shall maintain system logs to comply with applicable state and federal laws, rules, regulations, Departmental policies, and relevant ethical principals.

14.3. Management Review. ODH management reserves the right to examine at any time, and without prior notice, electronic mail messages, and files on personal computers, web browser cache files, web browser bookmarks, and other information stored on or passing through ODH resources. Such management access assures

compliance with internal policies, assists with internal investigations, and with the management of ODH information systems. ODH management may routinely review web sites visited, files downloaded, time spent on the Internet, and related information from IT resources. Through requests placed to the ODH OMIS Helpdesk, managers may receive reports of such information and use it to determine what types of Internet usage are appropriate for their area's business activities.

14.4. Blocking Sites. ODH may employ firewalls to routinely prevent users from connecting with certain non-business web sites. ODH staff that discovers he or she has connected with a web site that contains sexually explicit, racist, violent, or other potentially offensive material must immediately disconnect from that site and notify their ODH staff supervisors and project managers. ODH management will assess the event according to Ohio IT Policy ITP-B.7 (Security Incident Response). The ability to connect with a specific web site does not imply that users of ODH systems are permitted to visit that site.

15. Reporting Security Problems.

15.1. Notification Process. To ensure security, ODH equipment should not be used by ODH staff when conducting non-ODH business activities unless having received prior authorization from the Chief of OMIS. If non-public ODH information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Chief of MIS, the appropriate Office or Division Chief and the Office of the General Counsel must be notified immediately. If any unauthorized use of ODH's information systems has taken place, or is suspected of taking place, the Chief of OMIS must likewise be notified immediately. Ohio Revised Code section 1347.12 requires that ODH contact potentially impacted individuals residing in Ohio if unencrypted or unredacted personal information could cause identity fraud or other fraud. In accordance with Ohio IT Policy ITP-B.7 (Security Incident Response), security incident recovery procedures shall ensure IT security incident response (IR) capability based on a periodic risk assessment of data, processes, systems and networks. Systems shall have security notification features and related management controls must be in place as described in Ohio IT Policy ITP-B.10 (Security Notifications).

Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the ODH OMIS Helpdesk must be notified immediately. Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like should be reported to the ODH OMIS Helpdesk. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

15.2. False Security Reports. The Internet has been plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of chain letters that request that the receiving party send the message to other people. ODH staff in receipt of information about system vulnerabilities should forward it to the Chief of OMIS or designee, who will then determine what if any action is appropriate. ODH staff must not personally redistribute system vulnerability information.

15.3. Testing Controls. ODH staff shall not test or probe security mechanisms at an ODH site nor use ODH resources to test or probe security mechanisms at other Internet sites. The possession on ODH property of software tools for "cracking" information security is likewise prohibited. By written memorandum, the Chief of OMIS may grant an exception to this prohibition.

16. Violations of Systems Security Measures.

16.1. Confidentiality Procedures. Using IT resources to violate or attempt to circumvent confidentiality procedures by ODH staff is strictly prohibited.

16.2. Accessing or Disseminating Confidential Information. Accessing or disseminating confidential information or information about another person without authorization by ODH staff is strictly prohibited.

16.3. Accessing Systems without Authorization. Accessing networks, files or systems or an account of another person without proper authorization by ODH staff is strictly prohibited. Public servants such as ODH staff are individually responsible for safeguarding their passwords in accordance with Ohio IT Policy ITP-B.3 (Password and Personal Identification Number Security).

16.4. Distributing Malicious Code. Intentionally distributing malicious code or circumventing malicious code security by ODH staff is strictly prohibited. Ohio IT Policy ITP-B.4 (Malicious Code Security) outlines requirements for protecting IT resources against threats from malicious code. All ODH employees, contractors, temporary personnel and other ODH agents shall comply with Ohio IT Policy ITP-B.4 (Malicious Code Security).

Procurement processes shall contain assurance (including, but not limited to, contract terms) that software or other deliverables are free from known malicious code.

17. Penalties. Violation of this policy may result in disciplinary action or contractual penalties, and may be cause for termination. In addition, violations may result in investigation by law enforcement, civil action or criminal prosecution. The Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

- ORC Section 1347.99 – Personal information systems penalties.
- ORC Section 2909.04(B) – Knowingly using a computer, computer system, network, telecommunications device, other electronic devices or the Internet to disrupt or impair a government operation.
- ORC Section 2909.05(B)(2) – Causing serious physical harm to property that is owned, leased, or controlled by a government entity.
- ORC Section 2913.04 – Accessing any computer, computer system, or computer network without consent of the owner.
- ORC Sections 2921.41(A)(1) & 2921.41(A)(2) – Using a public office to commit theft, which includes fraud and unauthorized use of government computer systems.

18. Compliance. ODH will undertake measures to ensure that all staff (employees, contractors, temporary workers, students, student interns, volunteers, and other agents of

the state who use and administer ODH resources) adhere to agency policy. Contractors shall abide by state and agency security policies and practices as a condition of performance.

19. Awareness. ODH management will establish information technology education and awareness programs and shall ensure all employees, contractors, temporary personnel and other agents of the state adhere to the programs' content in accordance with Ohio IT Policy ITP-B.8 (Security Education and Awareness).

20. State Registry. ODH has submitted to the Ohio Office of Information Technology Investment and Governance Division Statewide IT Policy Program Area ("Statewide IT Policy") a copy of its policy.

21. Authority. This directive is promulgated by the Director of Health pursuant to Ohio Revised Code sections 121.02, 121.07, 1347, 3701.03 and 3701.04, which authorize the Director to create, promulgate and enforce rules for the safe, efficient, economic and proper operation of the agency. In addition, the Director has parallel authority under Article 5 of the OCSEA and 1199 contracts as well as Article 3 of the OEA contract. An additional reference is DAS Directive 00-26.

Approved: Alvin Jackson, M.D.
Director

Date: 6-30-2009

Table of Effective Changes

Version	Effective Date	Superseded/Modified	Significant Changes
Directive 402	12/01/2001	NA	First issuance
Directive 402a	07/01/2003	402	Authorized use of resources for off-duty educational purposes
Directive 7	07/31/2006	402a	Update to new format specified by ODH Directive 1; in accordance to OIT Policy ITP-E.8
Directive 7A	10/11/2007	7	Update to Directive 7 in accordance with new OIT and ODH policy updates
7B	06/30/2009	Directive 401 Directive 601 Directive 1202 OMIS Letter 2 OMIS Letter 3 OMIS Letter 4 OMIS Letter 5 7A	Consolidation of similar policies and revisions in accordance with new O.R.C. (predominately 1347), OIT and ODH policy updates

Ohio Department of Health
Information Technology Code of Responsibility

Each Ohio Department of Health (ODH) staff member (employees, contractors, temporary workers, students, student interns, volunteers, and other agents of the state who use and administer ODH resources) using an ODH owned or provided computer system or network holds a position of trust relative to information contained or stored in such system or network and must recognize the responsibilities entrusted to him/her in preserving the security and confidentiality of the systems and their contents. Confidentiality requirements contained in law include, but are not limited to: 45 Code of Federal Regulations 164.501 et al. (HIPAA); Ohio Revised Code sections 2301.35, 5101.25, 5101.27, 5101.28, 5101.29, 5101.30; and Ohio Administrative Code sections 5101:1-1-03 and 5101:1-29-071.

Therefore, any staff member of ODH, or any person with authorized access to the computer system by or for ODH:

(1) Shall not operate or request others to operate any computer and/or related equipment in any manner prohibited or not authorized by ODH Directive 7B (Policy on the Use and Security of the Agency IT);

(2) Shall not "flame" or make similar written attacks, including threats against another user or organization, over ODH IT systems. All messages that might be perceived to harass, annoy or alarm another person or organization are similarly prohibited. ODH staff will not use ODH IT systems to transmit or download material that is defamatory, racially or sexually harassing, threatening, obscene, pornographic, or which may contribute to a hostile work environment. ODH staff will not use the ODH IT systems to transmit or download material that would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability;

(3) Shall not use the ODH IT systems for operating a business for personal gain, non-work audio programs such as radio stations, sending chain letters, or soliciting money for religious or political causes;

(4) Shall not make or permit unauthorized use of information contained in any files maintained by the state or exhibit or divulge the contents of any records to any person except in the conduct of his/her work assignment, as required by law, or in accordance with the policies of the Ohio Department of Health, remove or cause to be removed copies of any official record or report from any file except in the performance of his/her duties; or knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry;

(5) Shall not make or permit unauthorized use of any computers owned, rented, authorized, or otherwise controlled by the state;

(6) Shall not seek to benefit personally or permit others to benefit personally, by any confidential information that has come to him/her by virtue of his/her work assignment;

(7) Shall not make copies of software or computer literature in violation of copyright laws;

(8) Shall report any violation of this Code of Responsibility or ODH Directive 7B (Policy on the Use and Security of the Agency IT Resources) by anyone to his/her supervisor immediately.

For state employees, VIOLATION OF THIS CODE OF RESPONSIBILITY OR ODH DIRECTIVE 7 (POLICY ON THE USE AND SECURITY OF THE AGENCY IT RESOURCES) MAY RESULT IN DISCIPLINARY ACTION UP TO AND INCLUDING REMOVAL. Any activity or conduct outside the scope of employment that may threaten the security and confidentiality of ODH electronic information, data systems, and/or wide area network may also be cause for disciplinary action.

For non-state employees, violation of the Code of Responsibility may result in denial of access to all ODH computer systems and programs and could result in criminal charges being filed.

I HAVE READ, UNDERSTAND AND AGREE TO ABIDE BY ALL PROVISIONS OF THE OHIO DEPARTMENT OF HEALTH INFORMATION TECHNOLOGY CODE OF RESPONSIBILTY AND ODH DIRECTIVE 7B (POLIC Y ON THE USE AND SECURITY OF THE AGENCY IT RESOURCES).

Signed: _____ (Employee Signature)

Signed: _____ (Print Employee Name)

Date: _____

Enclosure (1) of ODH Directive 7B
HEA 6200 (09/01/2011)

Request for Academic Use of ODH Computer Resource*

Pursuant to ODH Directive 7B, I hereby request permission to use ODH computer resources to assist me in completing the requirements of the below listed class or classes. I have read and fully understand the provisions of ODH Directive 7B and will comply with them. I understand that permission to use ODH computer resources during non-work hours is limited to those uses directly related to the coursework listed below.

Name (Print or Type): **Date:**

Bureau:

Academic Institution or Training Center:

Course (Name and Number)	Start Date	Finish Date

_____
Employee Signature

_____ _____
Bureau Chief Approval Signature **Date**

***Enclosure (2) of ODH Directive 7B**

HEA 0302 (Updated 07/2009)