ARKANSAS DEPARTMENT OF MILITARY
INFORMATION TECHNOLOGY AGREEMENT

TERMS OF INFORMATION TECHNOLOGY AGREEMENT

The terms of this agreement must be read in conjunction with any policy and any additional guidance provided by the Arkansas Department of Transformation and Shared Services and the Arkansas Department of the Military (DOTM). Signatories certify they will abide by this agreement and all supplemental terms established by the DOTM.

Network Acceptable Use Policy

The DOTM is committed to protecting all employees, partners, and the State of Arkansas from illegal or damaging actions by individuals, either knowingly or unknowingly. In furtherance of its commitment, the DOTM publishes this security awareness and acceptable use policy. The DOTM's intention for publishing a security awareness and acceptable use policy is not to impose restrictions that are contrary to the established culture of openness, trust, and integrity. Any list included in this policy is by no means exhaustive but an attempt to provide a framework for activities which fall into the category of unacceptable use.

Internet/Intranet-related systems provided by DOTM, including but not limited to computers, laptops, tablets, PDAs, wireless technology, operating systems, applications, removable electronic media, network accounts providing electronic email, Internet browsing, and remote access, are the property of DOTM. These resources are to be used for business purposes in serving the interests of the company and of our clients and customers during normal operations.

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

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at DOTM, including all personnel affiliated with third parties. This policy applies to all equipment, networks, systems, software, and other resources owned or leased by DOTM.

General Use and Ownership

1. While the IT Department desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of DOTM. Because of the need to protect the network, management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to DOTM.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet systems. Absent such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. DOTM equipment, systems, email address, etc. are not to be used to pursue outside business activities not sanctioned by the State of Arkansas.
4. The IT Department recommends that any information that users consider sensitive or vulnerable be encrypted.
5. For security and network maintenance purposes, authorized individuals within the DOTM may monitor equipment, systems, and network traffic at any time.
6. The DOTM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. Employees should take all necessary steps to prevent unauthorized access to confidential information, including, but not limited to, credit card information, personal information, state strategies, trade secrets, specifications, employee personal information, vendor and research data, and email and communications activities.
2. All passwords must be kept secure, and the sharing of accounts is prohibited. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed according to the Password Policy.
3. All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Employees should secure their workstations by logging off or locking them when the station will be unattended.
5. Use encryption of information when appropriate.
6. Information contained on portable computers is especially vulnerable; therefore, special care should be exercised.
7. Postings by employees from a state email address to newsgroups or social media are not allowed, unless posting is expressly authorized in furtherance of the agency's mission.
8. All computers used by the employee that are connected to the DOTM Internet/Intranet, whether owned by the employee or DOTM, shall be equipped with continually executing approved virus-scanning software with a current virus database.
9. Use extreme caution when opening e-mail attachments from unknown senders, which may contain viruses and/or other malware.
10. Classified systems and files are approved under strict configuration guidelines. Users are prohibited from making any changes to system settings, installing software applications or utilities, or modifying/changing system hardware or sharing of these files.

Unacceptable Use

The following activities are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of DOTM authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DOTM-owned resources.

1. Sending, forwarding, or requesting email with any type of confidential data such as credit card data. Any exceptions must be approved by the IT Department.
2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
3. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
4. Unauthorized use or forging of email header information.
5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited email originating from within DOTM's networks of other Internet/Intranet service providers on behalf of or to advertise any service hosted by DOTM or connected via DOTM's network.

8. Sending or forwarding email that is likely to contain computer viruses.
9. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DOTM.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DOTM or the end user does not have an active license is strictly prohibited.
3. Downloading and/or installing any type of software not related to job functions or not authorized by the IT Department. Drives will have to be encrypted and password protected.
4. Connecting network devices such as wireless access points or personal laptops into the DOTM network environment without proper authorization from the IT Department.
5. Connecting removable storage devices such as USB drives or external hard drives from a non-government agency. Non-government devices are not allowed unless approved by the IT department. Approved drives must be encrypted, and password protected.
6. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
7. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
8. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
9. Using a DOTM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
10. Making fraudulent offers of products, items, or services originating from any DOTM account.
11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this Acceptable Use Policy section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Port scanning or security scanning is expressly prohibited unless authorized by the IT Department.
13. Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
14. Circumventing, or attempting to circumvent, the user authentication or security of any host, network, or account.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/ Intranet.
17. Providing information about or lists of DOTM employees to parties outside the DOTM without written approval of management or as required by law.

Any employee found to have violated this policy may be subject to disciplinary actions, up to and including termination of employment.

TRAINING

1. **All employees of DOTM are required to finish the designated CYBER Security Training within the allocated time frame provided for completion.**
2. **Failure to participate in and complete the CYBER Security Training may lead to potential consequences such as loss of network access and account deactivation for users.**
3. **All DOTM employees possessing network and computer access will receive an email from KNOWBE4 with the link to the required training.**

EMPLOYEE ACKNOWLEDGEMENT

The signature below certifies the employee has read and understands the Information Technology Agreement.

Written Name _____ Date _____

Signature _____