**ADECA CED Division**

**CDBG-DR Grant Program for Hurricanes Sally and Zeta**

**Maintaining a Comprehensive Website Policy**

Pursuant to the U. S. Department of Housing and Urban Development’s Federal Register Notice of Grant Funds to Address Major Disasters Occurring in 2020 and 2021 (Hurricanes Sally and Zeta in the State of Alabama) published on February 3, 2022 in Volume 87, Number 23 on pages 6364-6392, HUD has several requirements pertaining to maintaining and using a comprehensive website for purposes of administering this grant. This information is at the links <https://www.govinfo.gov/content/pkg/FR-2022-02-03/pdf/2022-02209.pdf> and [2022-02209.pdf (govinfo.gov)](https://www.govinfo.gov/content/pkg/FR-2022-02-03/pdf/2022-02209.pdf). These requirements are stated as follows:

**Federal Register, February 3, 2022, Volume 87, No. 23**

|  |
| --- |
| **Federal Register, February 3, 2022, Volume 87, No. 23, at page 6366:**  *III.A.1.a. Publication of the action plan for program administrative costs and opportunity for public comment*.  The grantee must publish the proposed action plan for program administrative costs, and substantial amendments to the plan, for public comment. To permit a more streamlined process and ensure that grants for program administrative costs are awarded in a timely manner in order to allow grantees to more rapidly design and launch recovery activities, provisions of 42 U.S.C. 5304(a)(2) and (3), 42 U.S.C. 12707, 24 CFR 570.486, 24 CFR 1003.604, 24 CFR 91.105(b) through (d), and 24 CFR 91.115(b) through (d), with respect to citizen participation requirements, are waived and replaced by the alternative requirements in section III.A.1. that apply only to action plans for program administrative costs and substantial amendments to these plans. Additionally, for these action plans only, grantees are not subject to the Consolidated Notice action plan requirements in sections III.B.2.i., III.C.2., III.C.3., III.C.6., and III.D.1.a.–c. The manner of publication of the action plan for program administrative costs must include prominent posting on the grantee’s official disaster recovery website and must afford residents, affected local governments, and other interested parties a reasonable opportunity to review the contents of the plan or substantial amendment. Subsequent to publication of the action plan or substantial amendment to that plan, the grantee must provide a reasonable time frame (no less than seven days) and multiple methods (including electronic submission) for receiving comments on the action plan or substantial amendment for program administrative costs. At a minimum, the topic of disaster recovery on the grantee’s website, including the posted action plan or substantial amendment, must be navigable by interested parties from the grantee homepage and must link to the disaster recovery website as required by section III.D.1.e. of the Consolidated Notice. The grantee’s records must demonstrate that it has notified affected parties through electronic mailings, press releases, statements by public officials, media advertisements, public service announcements, and/or contacts with neighborhood organizations. Grantees are not required to hold any public hearings on the proposed action plan or substantial amendment for program administrative costs.  **Federal Register, February 3, 2022, Volume 87, No. 23, at page 6377:**  *III. Grant Administration*  *III.A. Pre-Award Evaluation of Management and Oversight of Funds*  *III.A.1. Certification of financial controls and procurement processes, and adequate procedures for proper grant management.*  *\* \* \**  *III.A.1.a. Documentation requirements.*  *\* \* \**  (5) Comprehensive disaster recovery website.  A grantee has adequate policies and procedures to maintain a comprehensive accessible website if it submits policies and procedures indicating to HUD that the grantee will have a separate web page dedicated to its disaster recovery activities assisted with CDBG-DR funds that includes the information described at section III.D.1.d.–e. The procedures must also indicate the frequency of website updates. At minimum, grantees must update their website quarterly.  **Federal Register, February 3, 2022, Volume 87, No. 23, at page 6383:**  *III.C. Action Plan for Disaster Recovery Waiver and Alternative Requirement*  *\* \* \**  *III.C.6. Amending the action plan.*  The grantee must amend its action plan to update its needs assessment, modify or create new activities, or reprogram funds, as necessary, in the DRGR system. Each amendment must be published on the grantee’s official website and describe the changes within the context of the entire action plan. A grantee’s current version of its entire action plan must be accessible for viewing as a single document at any given point in time, rather than require the public or HUD to view and cross-reference changes among multiple amendments. HUD’s DRGR system will include the capabilities necessary for a grantee to sufficiently identify the changes for each amendment. When a grantee has finished amending the content in the Public Action Plan, the grantee will click ‘‘Submit Plan’’ in the DRGR system. The DRGR system will prompt the grantee to select the ‘‘Public Action Plan’’ and identify the amendment type (substantial or non-substantial). The grantee will complete this cover page to describe each amendment. At a minimum, the grantee must: (1) Identify exactly what content is being added, deleted, or changed; (2) clearly illustrate where funds are coming from and where they are moving to; and (3) include a revised budget allocation table that reflects the entirety of all funds, as amended.  *III.C.6.a. Substantial amendment*.  In its action plan, each grantee must specify criteria for determining what changes in the grantee’s plan constitute a substantial amendment to the plan. At a minimum, the following modifications will constitute a substantial amendment: A change in program benefit or eligibility criteria; the addition or deletion of an activity; a proposed reduction in the overall benefit requirement, as outlined in III.F.2.; or the allocation or reallocation of a monetary threshold specified by the grantee in their action plan. For all substantial amendments, the grantee must follow the same procedures required for the preparation and submission of an action plan for disaster recovery, with the exception of the public hearing requirements described in section III.D.1.b. and the consultation requirements described in section III.D.1.a., which are not required for substantial amendments. A substantial action plan amendment shall require a 30-day public comment period.  **Federal Register, February 3, 2022, Volume 87, No. 23, at page 6384:**  *III.D. Citizen Participation Requirements*  *III.D.1. Citizen participation waiver and alternative requirement.*  *\* \* \**  *III.D.1.b. Publication of the action plan and opportunity for public comment.*  Following the creation of the action plan or substantial amendment in DRGR and before the grantee submits the action plan or substantial amendment to HUD, the grantee must publish the proposed plan or amendment for public comment. The manner of publication must include prominent posting on the grantee’s official disaster recovery website and must afford citizens, affected local governments, and other interested parties a reasonable opportunity to review the plan or substantial amendment. Grantees shall consider if there are potential barriers that may limit or prohibit vulnerable populations or underserved communities and individuals affected by the disaster from providing public comment on the grantee’s action plan or substantial amendment. If the grantee identifies barriers that may limit or prohibit equitable participation, the grantee must take reasonable measures to increase coordination, communication, affirmative marketing, targeted outreach, and engagement with underserved communities and individuals, including persons with disabilities and persons with LEP. At a minimum, the topic of disaster recovery on the grantee’s website must be navigable by all interested parties from the grantee homepage and must link to the disaster recovery website required by section III.D.1.e. The grantee’s records must demonstrate that it has notified affected citizens through electronic mailings, press releases, statements by public officials, media advertisements, public service announcements, and/or contacts with neighborhood organizations.  *\* \* \**  *III.D.1.d. Availability and accessibility of documents*.  The grantee must make the action plan, any substantial amendments, vital documents, and all performance reports available to the public on its website. See the following guidance for more information on vital documents: https://www.lep.gov/ guidance/HUD\_guidance\_Jan07.pdf. In addition, the grantee must make these documents available in a form accessible to persons with disabilities and those with LEP. Grantees must take reasonable steps to ensure meaningful access to their programs and activities by LEP persons, including members of protected classes, vulnerable populations, and individuals from underserved communities. In their citizen participation plan, state and local government grantees shall describe their procedures for assessing their language needs and identify any need for translation of notices and other vital documents. At a minimum, the citizen participation plan shall require that the state or local government grantee take reasonable steps to provide language assistance to ensure meaningful access to participation by non-English-speaking residents of the grantee’s jurisdiction.  *III.D.1.e. Public website*.  The grantee must maintain a public website that permits individuals and entities awaiting assistance and the general public to see how all grant funds are used and administered. The website must include copies of all relevant procurement documents and, except as noted in the next paragraph, all grantee administrative contracts, details of ongoing procurement processes, and action plans and amendments. The public website must be accessible to persons with disabilities and individuals with LEP.  To meet this requirement, each grantee must make the following items available on its website: The action plan created using DRGR (including all amendments); each performance report (as created using the DRGR system); citizen participation plan; procurement policies and procedures; all contracts, as defined in 2 CFR 200.22, that will be paid with CDBG–DR funds (including, but not limited to, subrecipients’ contracts); and a summary including the description and status of services or goods currently being procured by the grantee or the subrecipient (e.g., phase of the procurement, requirements for proposals, etc.). Contracts and procurement actions that do not exceed the micro-purchase threshold, as defined in 2 CFR 200.1, are not required to be posted to a grantee’s website.  *III.D.1.f. Application status.*  The grantee must provide multiple methods of communication, such as websites, toll-free numbers, TTY and relay services, email address, fax number, or other means to provide applicants for recovery assistance with timely information to determine the status of their application.  *\* \* \**  *III.D.1.h. General requirements*.  For plan publication, the comprehensive disaster recovery website and vital documents must ensure effective communication for individuals with disabilities, as required by 24 CFR 8.6 and the Americans with Disabilities Act, as applicable. In addition to ensuring the accessibility of the comprehensive disaster recovery website and vital documents, this obligation includes the requirement to provide auxiliary aids and services where necessary to ensure effective communication with individuals with disabilities, which may take the form of the furnishing of the above referenced materials in alternative formats (24 CFR 8.6(a)(1)). When required by III.D.1.d., grantees must take reasonable steps to ensure meaningful access for individuals with LEP.  **Federal Register, February 3, 2022, Volume 87, No. 23, at page 6392:**  *V. Performance Reviews*  *\* \* \**  *V.C. Grantee Reporting Requirements in the DRGR System*  *V.C.1. DRGR-related waivers and alternative requirements.*  The Consolidated Notice waives the requirements for submission of a performance report pursuant to 42 U.S.C. 12708(a), 24 CFR 91.520, and annual status and evaluation reports that are due each fiscal year under 24 CFR 1003.506(a). Alternatively, HUD is requiring that grantees enter information in the DRGR system on a quarterly basis through the performance reports. The information in DRGR and the performance reports must contain sufficient detail to permit HUD’s review of grantee performance and to enable remote review of grantee data to allow HUD to assess compliance and risk.  At a minimum, each grantee must:  a. Enter its action plan and amendments as described in III.C.1, including performance measures, into the Public Action Plan in DRGR;  b. Enter activities into the DRGR Action Plan at a level of detail sufficient to allow HUD to determine grantee compliance (when the activity type, national objective, and the organization that will be responsible for the activity is known);  c. Categorize activities in DRGR under a “project”;  d. Enter into the DRGR system summary information on grantees’ monitoring visits and reports, audits, and technical assistance it conducts as part of its oversight of its disaster recovery programs;  e. Use the DRGR system to draw grant funds for each activity;  f. Use the DRGR system to track program income receipts, disbursements, revolving loan funds, and leveraged funds (if applicable);  g. Submit a performance report through the DRGR system no later than 30 days following the end of each calendar quarter. For all activities, the address of each CDBG–DR assisted property must be recorded in the performance report; and  h. Publish a version of the performance report that omits personally identifiable information reported in the performance reports submitted to HUD on the grantee’s official website within three days of submission to HUD, or in the event a performance report is rejected by HUD, publish the revised version, as approved by HUD, within three days of HUD approval.  The grantee’s first performance report is due after the first full quarter after HUD signs the grant agreement. Performance reports must be submitted on a quarterly basis until all funds have been expended and all expenditures and accomplishments have been reported. If a satisfactory report is not submitted in a timely manner, HUD may suspend access to CDBG–DR funds until a satisfactory report is submitted, or may withdraw and reallocate funding if HUD determines, after notice and opportunity for a hearing, that the jurisdiction did not submit a satisfactory report. |

ADECA, as the grantee/grant recipient of the CDBG-DR Grant funds for Hurricanes Sally and Zeta, must have adequate policies and procedures to maintain a comprehensive accessible website. For purposes of the HUD Secretary’s certification, a grantee has adequate procedures to maintain a comprehensive website if the following statements are true:

1. The policies and procedures indicate to HUD that the grantee will have a separate webpage dedicated to its disaster recovery activities assisted with CDBG-DR funds and meet all requirements in the applicable *Federal Register* notice(s). Note: The grantee’s policies and procedures must indicate that the required items will be on its website. The required items in Section III.D.1.e of the February 3, 2022 Federal Register Notice are:

• the action plan created using DRGR (including all amendments);

• each performance report (as created using the DRGR system);

• citizen participation plan;

• procurement policies and procedures;

• all executed contracts that will be paid with CDBG-DR funds as defined in 2 CFR 200.22 (including subrecipients’ contracts); and

• a summary including the description and status of services or goods currently being procured by the grantee or the subrecipient (e.g., phase of the procurement, requirements for proposals, etc.).

Contracts and procurement actions that do not exceed the micro-purchase threshold, as defined in 2 CFR 200.67, are not required to be posted to a grantee’s website. [Section III.A.1.a.(5) of the February 3, 2022 Federal Register Notice].

2. For items required in Section III.D.1.d of the Consolidated Notice to be available to the public on its website, the grantee will make these documents available in a form accessible to persons with disabilities and those with limited English proficiency. [Section III.A.1.a.(5) the February 3, 2022 Federal Register Notice].

3. The grantee will take reasonable steps to ensure meaningful access to their programs and activities by LEP persons, including members of protected classes, vulnerable populations, and individuals from underserved communities as described in Section III.D.1.d of the Consolidated Notice. [Section III.A.1.a.(5) the February 3, 2022 Federal Register Notice]

4. The grantee will update its website at least quarterly. [Section III.A.1.a.(5) the February 3, 2022 Federal Register Notice]

ADECA maintains a comprehensive website for the online dissemination of information pertaining to the Department’s programs and operations. ADECA’s website is [www.adeca.alabama.gov](http://www.adeca.alabama.gov). With regard to the operations of this website, ADECA adheres to the following policies:

(1) State of Alabama’s Information Technology Policy 630-02 regarding “System Use.”

(2) ADECA Usage Policy and Security Guide for Computers and Network Access, Version 6.0, effective February 1, 2016.

These documents are contained below.

**State of Alabama’s Information Technology Policy 630-02 regarding “System Use.”**

|  |
| --- |
| **STATE OF ALABAMA**  **Information Technology Policy**  **POLICY 630-02: SYSTEM USE**  Inappropriate use of State information technology (IT) resources exposes the State and its data to  risks including potential virus attacks, compromise of network systems and services, and legal  liabilities. Effective security is a team effort involving the participation and support of every employee  and affiliate who deals with information and/or information systems. It is the responsibility of every IT  user to know these rules and to conduct their activities accordingly. These rules are in place to  protect the employee, the State, and the State’s data.  **OBJECTIVE:**  Define acceptable and non-acceptable use of State-owned IT resources including systems and  devices, software, Internet, and communications capabilities including e-mail, instant messaging, and  social media.  **SCOPE:**  This policy applies to all Executive Branch agencies, boards, and commissions except those exempt  under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).  SYSTEM USE POLICIES  Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software,  operating systems, storage media, and network accounts providing electronic mail, Internet access,  and Web browsing are the property of the State of Alabama. These systems are to be used for  business purposes in serving the interests of the government and of the people it serves in the course  of normal operations.  **PERSONAL USE:**  Limited personal use of State-managed computing resources is anticipated; however, employees and  managers are responsible for exercising good judgment regarding the reasonableness of personal  use.  Agencies may create additional policies concerning personal use of State information systems, but no  agency policy may impose a lesser limitation on personal use than is prescribed by this policy.  **PROHIBITED ACTIVITIES:**  The following activities are prohibited when using State IT resources:   * Any activity that is illegal under local, state, federal or international law * Non-incidental personal use of State-managed computing resources * Activities in support of personal or private business enterprises * Unauthorized reproduction of copyrighted material * Violating the rights of any person or other legal entity protected by copyright, trade secret,   patent or other intellectual property laws, or similar laws or regulations, including, but not limited to, laws which protect against the installation or distribution of software products that are not appropriately licensed for use by the State   * Exporting software, technical information, encryption software, or technology, in violation of   international or regional export control laws   * Introducing malicious software (malware) into the network or systems (e.g., viruses, worms,   Trojan horses, logic bombs, etc.) within reason of user’s control   * Making fraudulent offers of products or services * Making statements of warranty, expressed or implied, unless part of normal duties * Accessing, possessing, or transmitting material that is in violation of sexual harassment or   hostile workplace laws in the user's local jurisdiction   * Accessing, possessing, or transmitting any sexually explicit, offensive, or inappropriate images   and/or text   * 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 within the scope of regular duties; potential disruptions include, but are not  limited to, port/IP scanning, packet sniffing, or IP spoofing)   * Conducting network, system, or application scanning without IT Manager prior approval * 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   * Circumventing user authentication or security of any host, network, or account * Interfering with or denying service to any user except in the course of assigned duties * 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 network   * Accessing web sites offering online gambling, games, and related information such as cheats,   codes, demos, online contests, role-playing games, traditional board games, game reviews,  and sites that promote game manufacturers  **EXCEPTIONS:**  Employees may be exempted from some of these restrictions in the course of their legitimate job  responsibilities (e.g., Investigative personnel may require access to web sites that are otherwise  restricted).  IT Managers or Agency Heads shall request exceptions from the appropriate authority (e.g., Network  Support, State IT Security Council, or Director, Information Services Division, Department of  Finance).  INTERNET ACCESS POLICIES  Access to the Internet is provided as a business and informational resource to support and enhance  the capability of Internet users to carry out their job responsibilities. Internet users are expected to  handle their access privileges in a responsible manner and to follow all Internet-related policies and  procedures.  The State reserves the right to access, monitor, or disclose all Internet activity as required in the  course of monitoring, auditing, or responding to legal processes or investigative procedures.  Users do not enjoy any right of personal privacy when using State-provided Internet services. All  records created as a result of using Internet services are government records. As such, these records  are subject to the provisions of state laws regarding their maintenance, access, and disposition.  Internet usage records may be public records under the Alabama public records laws and may be  made available to the public upon lawful request. If an agency deems their use of Internet services is  an exception to the public records laws, the Agency Head shall request exception through the State  Records Commission.  **It is the responsibility of the Agency Head or Agency IT Manager to:**  Ensure that each employee, agent, contractor, or other person utilizing Internet services has been  advised of and understands all policies and restrictions applicable to the use of such services.  Take appropriate managerial and/or disciplinary action for inappropriate uses of Internet services  by state employees or other persons accessing Internet services through that agency.  **INTERNET CONTENT MANAGEMENT:**  Use of State IT resources for the purpose of viewing, executing, or downloading content inappropriate  for official State business exposes the State and its data to risks including virus attacks, spyware and  other malware threats, compromise of network systems and services, and potential legal and liability  issues. To mitigate these risks, access to certain categories of Internet content is restricted (blocked).  By the authority of the Director, Information Services Division, Department of Finance, the following  categories of Internet content present a threat to the security of State systems or have been deemed  not necessary for conducting official State business and are therefore blocked:   * Games and Gambling * Malicious Websites * Nudity and Risqué * Phishing * Peer-to-Peer File Sharing * Pornography * Proxy Avoidance * Spam URLs   Any additional website(s) or category of sites not listed above may also be blocked if deemed a cyber  security risk.  Exceptions may be granted to access blocked web sites for individuals or agencies that have a  business need for access in order to do their jobs. Each request for access to a blocked web site  requires a legitimate business need and written approval of the agency head or IT Manager and the  Director, Information Services Division, Department of Finance.  E-MAIL USAGE POLICIES  To ensure the integrity and availability of e-mail system resources all electronic communications are  expected to comply with relevant Federal and State laws as well as State policies and standards. The  following requirements apply to the use of State-provided e-mail systems.  E-mail shall be distributed, stored, and disposed of based on the data content in accordance with  State information management requirements.  E-mail content created, stored, transmitted, or received using State resources are the property of the  State. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of email  content. Authorized State personnel may access, monitor, or disclose e-mail content for state  business purposes or to satisfy legal obligations.  **PERSONAL USE OF STATE E-MAIL:**  State e-mail systems are to be used for business purposes in serving the interests of the government  and of the people it serves; however, incidental, occasional personal use of State e-mail is permitted.  Employees and managers are responsible for exercising good judgment regarding the  reasonableness (frequency and duration) of personal use.  In accordance with The Code of Alabama, Section 36-25-5, state e-mail shall not be used for  “personal gain.”  Personal e-mail shall be deleted or saved separately from work-related e-mail.  Users are permitted to include personal appointments in their Outlook calendar to help eliminate  scheduling conflicts.  Users may store personal contact information in their Outlook contacts folder.  **PROHIBITED USES OF STATE E-MAIL:**  State e-mail systems shall not be used for the creation or distribution of any disruptive or offensive  messages, including offensive (vulgar or pornographic) content or offensive comments about a  person’s race, gender, age, appearance, disabilities, political beliefs, or religious beliefs and  practices. Employees who receive any e-mail with this content from any State employee should report  the matter to their supervisor immediately. Additional prohibited uses of e-mail are addressed in State  standards.  In addition, the following activities are prohibited:   * Sending or forwarding remarks and/or images considered obscene, offensive, racist, libelous,   slanderous, or defamatory (as defined, where applicable, in The Code of Alabama 1975)   * Using an individual State e-mail account to send or forward virus or malware warnings, security   advisories, terrorist alerts, or other official warning, alert, or advisory messages without prior  approval of the agency IT Manager, Agency Information Security Officer, or Chief Information  Security Officer (unless in the course of normal assigned duties)   * Sending unsolicited e-mail messages including junk mail, spam, or other advertising material to   individuals who did not specifically request such material except in the execution of normal  government information dissemination   * Postings to newsgroups by personnel using a State e-mail address unless in the course of   business duties   * Using State e-mail for personal or commercial ventures, religious or political causes,   endorsement of candidates, or supporting non-government organizations   * Sending or forwarding chain letters or joke e-mail * Disguising or attempting to disguise your identity when sending e-mail * Sending e-mail messages using another person’s e-mail account * Intercepting e-mail messages destined for others * Unauthorized use, forging, or attempting to forge e-mail header information or messages   **AUTO-FORWARDING STATE E-MAIL:**  To preclude inadvertent transmission of inappropriate information onto the Internet, auto-forwarding  shall not be used to send State e-mail to an Internet e-mail address.  **MASS E-MAIL:**  Material sent to group distribution lists must be relevant to the group being mailed and shall pertain to  State business and/or serve the interests of State employees or constituents.  **Message Content/Format:**  Message format may be text, HTML, or RTF and should not include attachments.  HTML or RTF format messages may contain artwork, but shall be limited to a single page.  Each message shall contain a signature block with the sender’s name, departmental affiliation,  office telephone number, and e-mail address.  Sender is responsible for all replies, responses, and complaints.  **Message Approval:**  It is the responsibility of the sender/requestor of a mass e-mail to obtain the necessary approval  from the person, group, or designated owner of the distribution list.  Authority to use the “all-employees” distribution list rests with the Governor’s office.  Approval authority for agency/organization-level groups (e.g., “ISD – All Users”) shall rest with the  manager or management team presiding over that group.  Message shall include a line indicating the State office that approved the mass e-mail.  **Message Transmission:**  Mass electronic mailings shall only be transmitted in the evenings (after 5pm).  **List Owner Responsibilities:**  Owners of group distribution lists shall develop and monitor compliance with written operating  procedures for the use of their lists. All list owners are encouraged to consider the benefits of  moderating or otherwise controlling access to large lists. This applies whether a list has been  created for one-time use or is maintained as a standing list.  INSTANT MESSAGING POLICIES  Instant Messaging (IM) is subject to many of the same threats as e-mail (known security holes,  information leaks, vulnerability to malware, etc.), and IM users are frequently the target of phishing  attempts. For these reasons the following policies shall apply to all IM communications.  IM shall be used only for business communications (it is not provided for personal use).  IM shall not be used to communicate sensitive or confidential information.  IM shall be limited to text messages only; IM file transfers shall be blocked.  IM is correspondence that creates a record that can be subpoenaed and used as evidence in  litigation or regulatory investigations; therefore, IM correspondence shall be retained in accordance  with applicable State data and record retention policies.  IM content, created, stored, transmitted, or received using State resources, is the property of the  State. Nothing in this policy shall be construed to waive any claim of privilege or confidentiality of IM  content. Authorized State personnel may access, monitor, or disclose IM content for any business  purpose or to satisfy legal obligations.  REMOVABLE STORAGE DEVICE POLICIES  Removable non-volatile storage devices (USB Flash drives, PC Cards, FireWire devices, MP3  players, camcorders, digital cameras, etc.) have the same vulnerabilities as disk media (malware,  data loss) but greater capacity, and could be used to infect an information system to which they are  attached with malicious code, could be used to transport sensitive data leading to potential  compromise of the data, and are frequently lost or stolen. Careful attention to the security of such  devices is necessary to protect the data they may contain. For these reasons the following  requirements apply to the use of removable storage devices.  No removable storage device shall be attached to a State information system unless approved by the  IT Manager.  The IT Manager shall maintain an inventory of all approved removable storage devices and ensure  controls are in place to protect the confidentiality, integrity, and availability of State data.  Removable non-volatile storage devices shall be secured, marked, transported, and sanitized as  required by State standards in the manner appropriate for the data category they contain.  Removable non-volatile storage devices shall, whenever possible, be formatted in a manner that  allows the application of Access Controls to files or data stored on the device.  Sensitive or confidential data shall not be stored on any removable non-volatile storage device unless  encrypted in accordance with applicable State standards. For devices that do not support encryption  of the storage media, sensitive and confidential data shall, as promptly as possible, be transferred to  a device that does support the required encryption and access controls. In the interim, the device  shall be securely stored apart from its storage media (whenever possible) and physical security must  be assured. Organizational procedures shall clearly define the handling requirements for such data  and devices, and device users shall be made aware of the risks and procedures.  Virus-scan all portable storage media (diskettes, CDs, USB drives, etc.) before files residing on the  media are transferred or accessed.  Maintain physical security of removable storage devices. Report immediately the loss or theft of any  device containing any State data.  User awareness training shall describe the risks and threats associated with the use of removable  storage devices, the handling and labeling of these devices, and a discussion of the devices that  contain persistent non-removable memory.  SOFTWARE LICENSING AND USE POLICIES  Under the provisions of U.S. copyright law, illegal reproduction of software can be subject to civil and  criminal penalties including fines and imprisonment. Therefore, all system users must use only  properly licensed software and must use that software in accordance with the terms and conditions of  the license agreement.  **Information Technology Users shall NOT:**   * Copy, download, nor install unlicensed software * Install personally-owned software onto State-managed computer systems * Install State-owned software on any non-State-owned computer systems, including home   computers, unless specifically authorized in the software license agreement  **Agency IT Managers shall:**   * Ensure only software that is licensed to the organization is installed and used * Ensure software is installed and used in compliance with the license agreements * Routinely perform software audits to ensure policy compliance * Remove any software found on State information systems for which a valid license or proof of   license cannot be determined  The term “software” includes the program, media, and licenses for all operating systems, utilities,  services, and productivity tools whether freeware, shareware, open source, off-the-shelf, or custom developed without regard to the system(s) on which it is installed (workstation, server, etc.).  SOCIAL MEDIA POLICIES  State agencies desiring to enhance their ability to communicate and interact with the public are  turning to social media technologies such as weblogs, wikis, Facebook©, Twitter©, etc.  As with most technologies, social media poses certain risks including but not limited to:   * Adverse impact to network bandwidth * Reputational risk to personnel, the agency, and the State * Potential exposure or leakage of sensitive or protected information (such as copyrighted   material, intellectual property, personally identifying information, etc)   * Potential avenue for malware introduction into the organization’s IT environment   The following policies are established to address and minimize these risks and define the allowable  and prohibited uses of social media technologies in the State IT environment.  **SOCIAL MEDIA USE:**  Organizations may utilize commercial social networking websites (such as Facebook and Twitter) or  integrate social media capabilities (such as a wikis or weblogs) into State-hosted websites.  **Information Services Division (ISD) Responsibilities:**  ISD will provide security awareness training to educate users about the risks pertaining to social  media and social networking, and provide best practices for risk remediation.  **Agency Management Responsibilities:**   * Conduct a formal assessment of the risk resulting from agency use of social media   technologies.   * Assign appropriate personnel (Public Information Officer) to oversee the use of agency social   media, evaluate and authorize agency requests for usage, and determine appropriateness of  the content posted to social media sites.   * Understand that social media website contents are public records that must be retained and   archived in accordance with applicable agency records disposition requirements.   * Obtain ISD approval before integrating social media capabilities on any websites hosted,   developed, or administered by ISD.   * Periodically review social media usage to ensure it continues to reflect the agency’s   communication strategy and priorities.  **Agency IT or Website Administrator Responsibilities:**   * Disable (if possible) any unnecessary functionality within social media websites or applications,   such as instant messaging (IM) and file upload/exchange.   * Minimize or eliminating links to other websites, such as “friends”, to minimize the risk of   exposing a government user to a link that leads to inappropriate or unauthorized material.   * Suppress any commercial or third-party advertisements (sometimes present when using   freeware versions of social media software or tools).   * Monitor (and filter as necessary) all social media website content posted and/or viewed. * Prohibit/block file uploads to the maximum extent possible. Where file uploads are allowed,   ensure all user-submitted files are automatically virus scanned.   * Include appropriate statements on State-hosted social media sites advising users of the public   nature of the information they post.  **User Responsibilities:**   * Social media may not be used for personal gain, conducting private commercial transactions,   or engaging in private business activities.   * Understand that postings to social media websites immediately become part of a public record. * Users shall not post or release proprietary, confidential, sensitive, personally identifiable   information (PII), or other state government Intellectual Property on social media sites.   * Users who connect to social media websites through State information assets, who speak   officially on behalf of the state agency or the State, or who may be perceived as speaking on  behalf of an agency or the State, are subject to all agency and State requirements addressing  prohibited or inappropriate behavior in the workplace, including acceptable use policies, user  agreements, sexual harassment policies, etc.   * Users shall not speak in social media websites or other on-line forums on behalf of an agency,   unless specifically authorized by the agency head or the agency’s Public Information Office.   * Users may not speak on behalf of the State unless specifically authorized by the Governor. * Users who are authorized to speak on behalf of the agency or State shall identify themselves   by: 1) Full Name; 2) Title; 3) Agency; and 4) Contact Information, when posting or exchanging  information on social media forums, and shall address issues only within the scope of their  specific authorization.   * Users who are not authorized to speak on behalf of the agency or State shall clarify that the   information is being presented on their own behalf and that it does not represent the position of  the State or an agency.   * Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or   credentials except for legitimate law enforcement purpose or for other legitimate State  purposes as defined in agency policy.   * Users shall use different passwords for different accounts; do not use the same password for   both a social media site and state network or e-mail accounts.  **Personal Use of Social Media Sites:**   * Employees may use personal social media for limited family or personal communications   during normal business hours so long as those communications do not interfere with their work.  Employees and their managers are responsible for exercising good judgment regarding  personal use.   * Users shall not use their state e-mail account or password in conjunction with a personal social   media site.  **Additional Recommended Security Measures:**  For added security, all users of Facebook are encouraged to enable SSL activation in their Facebook  account settings.  POLICY ENFORCEMENT  **REPORTING:**  Users should report security-related issues and policy non-compliance to their immediate supervisor,  manager, or as outlined in the applicable information security policy, standard, or procedures.  **NON-COMPLIANCE:**  Employee conduct or behavior while using any State-managed information system must comply with  ISD information security policies. Violation can result in disciplinary action up to and including  termination. Conduct or communications which violate State or Federal laws will not only be grounds  for immediate termination, but may also subject the employee to criminal prosecution. Suspected  violators of any laws, including copyright laws and FCC regulations, involving information services  provided by the State of Alabama will be reported to the appropriate agency head and/or the Attorney  General of Alabama for investigation and appropriate legal action. Some policy non-compliances may  be punishable under The Code of Alabama 1975 (Section 13A-8-100 through 13A-8-103), Alabama  Computer Crime Act. Such cases will be referred to the appropriate authorities. Other policy non-compliances by users shall be handled in accordance with the applicable disciplinary guidelines  established by the user’s agency. ISD will determine on a case-by-case basis when policy noncompliance  is sufficient grounds to deny the user access to information services.  **ADDITIONAL INFORMATION:**  Information Technology Dictionary  http://cybersecurity.alabama.gov/documents/IT\_Dictionary.pdf  *By Authority of Director, Information Services Division, Department of Finance* |

**ADECA Usage Policy and Security Guide for Computers and Network Access, Version 6.0, effective February 1, 2016.**

|  |
| --- |
| **ADECA**  **Usage Policy and Security Guide**  **for**  **Computers and Network Access**  **Version 6.0**  **February 1, 2016**  **Prepared by:**  **Alabama Department of Economic and Community Affairs**  **Information Services Section**  **Montgomery, Al.**  **ADECA**  **Usage Policy and Security Guide**  **for**  **Computers and Network Access**  **TABLE OF CONTENTS**  1.0 General Policies 324  1.1 General 324  1.2 Securing Agency Owned Computer Resources 325  1.3 System Administrator Requirements 325  1.4 Adherence to Terms of Software Licenses and Agreements 325   1. Limitations on Use of Agency Computer Resources………………………………………………………………………….5 2. Consent to Monitoring to Confirm Unauthorized Use of Agency Computer Systems and   Networks 325  1.7 Prohibition of Use of Social Security Numbers to Identify Records of Individuals 326  1.8 Protection of Privacy of Employee Records 326  1.9 User Access of Computer Systems 326  2.0 User Responsibilities 326  2.1 General 326  2.2 Responsibilities 326  3.0 User Management Responsibilities 327  3.1 Definition of user management 327  3.2 Responsibilities 327  4.0 Security Administrator Responsibilities 327  4.1 Definition of security administrator 327  4.2 Responsibilities 327  5.0 Systems Development Responsibilities 328  5.1 Definition of systems development 328  5.2 Responsibilities: 328  6.0 Back-up and recovery 328  7.0 Safeguarding of Computer Hardware 328  8.0 Safeguarding of Computer Software 328  8.1 Backup and usage 328  8.2 Copyright Laws/Proprietary Software 329  8.3 Safeguarding of Computer Program Documentation 329  8.4 Limitations on copying commercial software documentation 329  8.5 Copying of documentation for locally developed reports and custom Applications 329  9.0 Safeguarding of Computer Data 329  9.1 Restricting access to sensitive data 329  9.2 Destruction of sensitive data 330  10.0 Computer Networks & Configuration  Responsibilities………………………………………………………………..…10  10.1 General 10  10.2 Definition 11  10.3 Primary networking equipment 11  10.4 Secondary networking equipment 11  10.5 Lack of privacy/security of certain information on networks 11  10.6 Network Address Assignments 11  10.7 Inter-Departmental Applications, Network Attachments, Including LANs and WANs.…............................................................................................................................11  11.0 Password Administration 12  11.1 General 12  11.2 Recording and creating passwords 12  12.0 Security Violation Administration 12  12.1 General 12  APPENDIX A 13  APPENDIX B 21  **COMPUTER NETWORK SECURITY AND ACCEPTABLE USAGE POLICY** 1.0 General Policies*1.1 General* 1.1.1. Definitions:  1.1.1.1. User - any person utilizing agency computing resources.  1.1.1.2. Agency computing resources - any agency owned or controlled hardware, software, networking device, service or product.  1.1.2. The agency relies heavily on the use of electronic data processing systems and computers to meet its operational, financial, and informational requirements in an efficient manner. It is essential that its systems and equipment be protected from misuse, and unauthorized access. It is also essential that the agency computers, and the data that they store and process, be operated and maintained in a secure environment.  1.1.3. Allagency employees and authorized users of agency computer and network facilities are required to comply with the State of Alabama Information Technology Policy (which is included in this document as Appendix A), and the Computer Network Security and Acceptable Usage Policies in this document. All agency employees are required to read these documents and sign the **ADECA Employee Computer Policy Consent Form** in Appendix B.  1.1.4. A User who intentionally and without proper authorization, directly or indirectly, accesses, damages or destroys any computer, computer system, computer network, program, or data, or causes any such acts to occur, will be subject to adverse action. In the case of agency employees**,** suchadverse action may include termination of employment. In cases where such activities violate State or Federal criminal statutes, violations (whether committed by agency employees or others with no such connection to the agency) may be reported to appropriate law enforcement authorities for investigation and prosecution.  1.1.5. A User who utilizes the agency provided computer equipment, including network facilities, for any purposes other than for official agency purposes, is guilty of misuse of State resources, and is subject to both agency personnel action and appropriate criminal prosecution.  1.1.6. Agency management may, with prior evidence of misuse, both monitor and limit incoming and outgoing electronic messages to insure compliance with all legal requirements and agency policies. The unauthorized use of any agency computer and network resources may be subject to termination of computer services, and other appropriate agency personnel and State Code action.  1.1.7. **All Users of agency computers with network connectivity must read this document and sign the Employee Consent Form in the appendix of this document. Any use of agency computers with network capabilities by persons who have not signed the Employee Consent Form, constitutes prima facie evidence of unauthorized use of agency computer and network facilities and will be subject to discipline or prosecution, or both, as specified in this policy.** *1.2 Securing Agency Owned Computer Resources* 1.2.1 All computer equipment, including personal computers, minicomputers, mainframe computer systems, smart phones, tablets, removable media, software, files, and computer generated reports are assets of the agency and must be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based. *1.3 System Administrator Requirements* 1.3.1 All computer assets are assigned to a responsible party. Each application system, and its associated programs and files, are assigned a system administrator who is responsible for ensuring that adequate controls and procedures are in place to protect the integrity of the resources. These controls include application design, testing, computer access security, and proper usage and disposal. *1.4 Adherence to Terms of Software Licenses and Agreements* 1.4.1 All Users provided access to agency computers must adhere strictly to the terms, conditions, and limitations contained in the software licenses and agreements relating to computer software used on any agency computer. *1.5 Limitations on Use of Agency Computer Resources* 1.5.1 All agency computer resources, including personal computers, mini-computers, mainframe computer systems, smart phones, tablets, removable media, software, files, and computer generated reports may be used only for authorized purposes in support of official functions of the agency. *1.6 Consent to Monitoring to Confirm Unauthorized Use of Agency Computer Systems and Networks* 1.6.1 Any individual who utilizes any agency computer resource consents by that use to monitoring of such use. *1.7 Prohibition of Use of Social Security Numbers to Identify Records of Individuals* 1.7.1 Social Security Numbers will not be used to identify computerized records of any individual except to the extent that such use is permitted by the Privacy Act (5 U.S. Code 552a). *1.8 Protection of Privacy of Employee Records*  1. The policies and procedures of the agency will respect the privacy of employee records as defined in the Privacy Act (5 U.S. Code 552a).  *1.9 User Access of Computer Systems* 1.9.1 Allusers are held accountable for all actions performed on the computer systems with their log-on ID (i.e., user name and password).  1.9.2 Users are only to perform functions on the computer systems for which they are authorized and only to the extent that they have been authorized.  1.9.3 Any of the following constitute a violation of agency policy:  1.9.3.1 Deliberate, unauthorized attempts to access or use the agency computers, computer facilities, networks, systems, programs, or data or the unauthorized manipulation of the agency computer systems, programs, or data.  1.9.3.2 Deliberate, unauthorized use of agency facilities or equipment to access non-agency computers.  1.9.3.3 Deliberate, unauthorized activity that causes agency computers, computer facilities, systems, programs, or data to be accessed or used. 2.0 User Responsibilities*2.1 General* 2.1.1 Users, user management, security administrators, and systems development are all responsible for maintaining security controls. The following delineates their specific duties and responsibilities. *2.2 Responsibilities* 2.2.1. All users are responsible for adoption and active support of security procedures, including:  2.2.1.1. Keeping their user ID and password confidential;  2.2.1.2. Reporting all known security exposures and violations to their supervisor or senior manager, or the head of the agency Information Services section; and  2.2.1.3. Using agency computers and computer systems only in support of their authorized job responsibilities or consistent with the limitations of the permission granted them (in the case of all users). 3.0 User Management Responsibilities*3.1 Definition of user management* 3.1.1 User management are those persons who facilitate computer resources, issue user IDs and passwords, and are responsible for overseeing the use of computer systems. *3.2 Responsibilities* 3.2.1 Reviewing and approving all requests for changing their employee's access authorizations;  3.2.2 Initiating security change requests to keep employees' security records current with their positions and job functions, including termination and transfers;  3.2.3 Providing employees with the training needed to properly use the computer systems; and  3.2.4 Reporting any known security violations to the Agency management. 4.0 Security Administrator Responsibilities*4.1 Definition of security administrator*  1. The Security Administrator is an agency designated individual responsible for both the security policies of all agency computer/network resources and the agency's internal compliance with the Usage Policy and Security Guide.  *4.2 Responsibilities* 4.2.1 Providing basic security support for all systems;  4.2.2 Advising in the implementation of security controls on all systems, from the point of system design, through testing and production implementation;  4.2.3 Providing comprehensive information about security controls affecting system users and application systems;  4.2.4 Providing security support for all system users;  4.2.5 Maintaining the agency Usage Policy and Security Guide;  4.2.6 Maintaining state of the art equipment to confirm and document misuse of agency computer and network resources.  4.2.7 Serve as the agency working contact with Local, State, and Federal Agencies in instances of agency employee violation of the Usage Policy and Security Guide; and   1. Report Usage Policy and Security Guide violations to the head of the agency Information Services section.  5.0 Systems Development Responsibilities*5.1 Definition of systems development* 5.1.1 The Systems Development section designs and develops custom software applications for the various computer platforms deployed in the agency. Systems Development is responsible for including reasonable security and back-up controls in the applications being developed and maintained, including: *5.2 Responsibilities:* 5.2.1 Providing assistance in the identification and classification of computer resources;  5.2.2 Working with user areas and security administration to develop and integrate security controls into all systems, from the point of system design, through testing and production implementation;  5.2.3 Creating comprehensive documentation on application design, program logic, back-up and recovery procedures, internal application security controls and interdependence on other systems; and  5.2.4 Thoroughly testing all systems for accuracy and for proper security and disaster recovery controls. 6.0 Back-up and recovery 6.1 For centralized systems, the System Administrator must ensure that recovery systems are in place so that all critical applications and data are recoverable without seriously hampering operations. For personal computer applications, this is the responsibility of the individual computer user. 7.0 Safeguarding of Computer Hardware 7.1 Treat your computer equipment as you would any piece of delicate equipment that you depend on.  7.2 Know the model, serial number, and key characteristics of your equipment.  7.3 Do not allow the machine to be exposed to elements such as dust, smoke, and/or liquids that can easily harm the electronic circuitry. 8.0 Safeguarding of Computer Software*8.1 Backup and usage* 8.1.1 Only agency approved software is to be installed on agency computers. After the software is installed, the software's media should be kept in a safe, secure place that is separate from the computer equipment where the software is installed.  8.1.2 Unauthorized use of software will violate copyright or license agreements and can lead to personal financial liability as well as disciplinary action and criminal prosecution under federal and state law.  8.1.3 Unless specifically allowed by the software license, loaning the media of copyrighted software to others will constitute unauthorized use. *8.2 Copyright Laws/Proprietary Software* 8.2.1 All software must be used in strict compliance with the license or other agreement that sets out the terms and conditions of its use, all users must keep in mind that those terms vary.  8.2.2 Licenses for some software installed on a network limit the number of concurrent users, contact the Security Administrator for clarification.  8.2.3 Failure to comply with the usage restrictions contained in a software license or other agreement can result in agency and/or personal liability and may result in disciplinary action. Federal and state criminal prosecutions are also a possibility. *8.3 Safeguarding of Computer Program Documentation* 8.3.1 The best protection for your computer documentation is to store it in a secure, but easily accessible place. *8.4 Limitations on copying commercial software documentation* 8.4.1 For commercial or purchased software, copying documentation may be a copyright violation. **DO NOT** make any copies of vendor supplied documentation except as specifically authorized in the Software License agreement. If you have any questions regarding this policy, contact the Information Services Manager. *8.5 Copying of documentation for locally developed reports and custom Applications* 8.5.1 Documentation that supports a recurring report or custom application that has been developed within the department can, and should be, reproduced. A reproduction of the original should be labeled as the working copy that is used by users; and the original documentation should be stored in a separate location that is safe and secure from any chance of destruction. 9.0 Safeguarding of Computer Data*9.1 Restricting access to sensitive data* 9.1.1 The best protection for your data is to lock it up. Store your media, reports, etc. in a secure place. Log out, lock, or use a screen saver password for when you will be away from your computer. *9.2 Destruction of sensitive data* 9.2.1 When you no longer need printed reports or stored data on your hard disk, or external media, get rid of it by following one of the procedures below:  9.2.1.1 Shred and/or dispose of old reports that are no longer needed.  9.2.1.2 On a hard disk configuration, delete or erase unneeded files by using the file handling utilities of the application used to create the original file.   1. On external media, delete or erase unneeded files by using the file handling utilities of the application used to create the file. 2. Prior to taking computers, phones, tablets, and external media out of service, contact the Information Services Section to have the device electronically wiped.    10.0 Computer Networks & Configuration Responsibilities*10.1 General* 10.1.1 The agency network is owned by, and available to employees in the agency. Due to the nature of electronic data networking, the potential for harm to the entire network by one errant component is significant. The network will function only if everyone follows a set of basic guidelines for network access and use. All agency local and wide area network configurations must be approved and the overall configuration maintained by Information Services. Failure to coordinate these sub networks with Information Services can cause the entire network to become inoperable. *10.2 Definition* **10.2.1** The State network provides data communications for operations, research, and administrative applications. The primary internal network is Ethernet and supported protocols are TCP/IP. Attachments to the Ethernet backbone shall be made only by agency Information Services personnel using previously approved components. All primary networking equipment will be considered to be the management responsibility of Information Services. Once primary networking equipment is installed, it becomes the responsibility of Information Services and may not be relocated by the user department*.* *10.3 Primary networking equipment* 10.3.1 The network consists of primary and secondary networking equipment. Primary networking equipment is generally those pieces of equipment that are seen by the network as a "whole", including:  10.3.1.1 Fiber optic and LAN cabling.  10.3.1.2 Patch panels and premise wiring.  10.3.1.3 Transceiver taps and cables.  10.3.1.4 Active elements such as routers, bridges, repeaters, and gateways. *10.4 Secondary networking equipment* 10.4.1 Secondary networking equipment includes equipment that is logically on the "user" end of a bridge or gateway, such as workstations and Local Area Networks (LANs) and Wide Area Networks (WANs). *10.5 Lack of privacy/security of certain information on networks*  10.5.1 Because of the many access methods, types of storage devices, and backup routines, no data should be considered private or secure. The network user is responsible for the integrity and security of files and transmissions. *10.6 Network Address Assignments* 10.6.1 Only the Information Services group will assign Internet Protocol (IP) network addresses  **10.7 Inter-departmental applications, network attachments, including**  **LANs and WANs.**  10.7.1 Any inter-departmental network applications, network attachments (including LANs and WANs) must be coordinated with Information Services. Failure to comply with this network policy will result in removal of the offending equipment from the network. 11.0 Password Administration*11.1 General* 11.1.1 Passwords are to be kept confidential. Only the individual user to whom the log-on ID is assigned, Information Services personnel for maintenance purposes, and appropriate personnel as assigned by management, (see paragraph 11.2.1) are to know the password. Disclosure of the password to any other person(s) is a serious security violation and may result in loss of systems access privileges, and possible disciplinary actions. Use of "Password Saving" features in commercial software is strongly discouraged, since it defeats the purpose of password protection. In documented instances, it can permit the transmittal of objectionable material with the apparent author incorrectly identified. *11.2 Recording and creating passwords* 11.2.1 There sometimes arises a business need to access information stored on a computer during the assigned employee’s absence and in the event of an employee leaving the agency. Therefore, a list of passwords should be recorded by the division or section chief for the computers in their area. The division or section chief must ensure that this list is secured so that no one else has access to it. This can be accomplished by the division or section chief either by assigning a person as “Password Officer” for their area, or by assigning these duties to the immediate supervisor of each employee. Otherwise, passwords are not to be programmed into a computer, or recorded anywhere else that someone may find and use them. When creating a password, it is important not to use one that may be easily guessed, like a common dictionary word or name of a relative or pet. The best passwords are purely random combinations of letters, digits, numbers, and punctuation.  11.2.2 Passwords must be a minimum of 8 characters long and contain at least three of the following characteristics:   * Alphabetic characters * Numeric characters * Upper and lower case characters * Special characters  12.0 Security Violation Administration*General* 12.1.1 Security violations will be reported to the Information Systems Manager. |

|  |
| --- |
| **ADECA**  **EMPLOYEE COMPUTER POLICY CONSENT FORM**  I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. acknowledge that I have been provided a copy of the **ADECA USAGE POLICY AND SECURITY GUIDE FOR COMPUTERS AND NETWORK ACCESS** and the **STATE OF ALABAMA INFORMATION TECHNOLOGY POLICY.** 2. I certify that I have read these documents and agree to comply with all terms and conditions.      1. I understand that all network activity being conducted with state resources is the property of the State of Alabama. 2. I understand that the state reserves the right to monitor and log all network activity including e-mail, with or without notice, and therefore users have no right of personal privacy in the use of these resources. 3. I understand that misuse of computers and network resources constitutes misuse of state property, and can result in punitive action being taken against me including dismissal from state service.   Employee \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Return form to the ADECA Human Resources Manager) |

Pursuant to these documents, it is ADECA's policy that:

1. ADECA does have a separate webpage dedicated to its disaster recovery activities assisted with CDBG-DR funds, and it meets all requirements in the applicable *Federal Register* notice(s). This website is on the ADECA webpage [www.adeca.alabama.gov](http://www.adeca.alabama.gov) at the links <https://adeca.alabama.gov/cdbg-disaster-recovery/> and <https://adeca.alabama.gov/cdbg-disaster-recovery/hurricanes-sally-and-zeta/> and [Hurricanes Sally and Zeta – ADECA (alabama.gov)](https://adeca.alabama.gov/cdbg-disaster-recovery/hurricanes-sally-and-zeta/). In compliance with Section III.D.1.e of the February 3, 2022 Federal Register Notice, the following required items will be on ADECA's CDBG-DR website:

• ADECA's CDBG-DR Action Plan for CDBG-DR Grant for Hurricanes Sally and Zeta, created using DRGR (including all amendments);

• Each of ADECA's CDBG-DR performance reports (to be/as created using the DRGR system);

• ADECA's citizen participation plan;

• ADECA's CDBG-DR procurement policies and procedures;

• all of ADECA's executed contracts that will be paid with CDBG-DR funds as defined in 2 CFR §200.22 (including subrecipients’ contracts); and

• ADECA's summary - including the description and status of services or goods currently being procured by ADECA (as the grantee) or the subrecipient (e.g., phase of the procurement, requirements for proposals, etc.). ADECA notes that contracts and procurement actions that do not exceed the micro-purchase threshold, as defined in 2 CFR §200.67, are not required to be posted to ADECA (the grantee’s) CDBG-DR website [per Section III.A.1.a.(5) of the February 3, 2022 Federal Register Notice].

2. For items required in Section III.D.1.d of the February 3, 2022 Federal Register Notice to be available to the public on ADECA's website, ADECA (as the grantee) will make these documents available in a form accessible to persons with disabilities and those with Limited English Proficiency (LEP) [per Section III.A.1.a.(5) of the February 3, 2022 Federal Register Notice].

3. ADECA, as the grantee, will take reasonable steps to ensure meaningful access to ADECA's programs and activities by Limited English Proficiency (LEP) persons, including members of protected classes, vulnerable populations, and individuals from underserved communities as described in Section III.D.1.d of the February 3, 2022 Federal Register Notice [per Section III.A.1.a.(5) the February 3, 2022 Federal Register Notice].

4. ADECA, as the grantee, will update its website at least quarterly [per Section III.A.1.a.(5) the February 3, 2022 Federal Register Notice].

ADECA will follow these policies and procedures in its administration of the CDBG-DR Grant for Hurricanes Sally and Zeta.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ End of Maintaining A Comprehensive Website Policy \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_