Murray Electric Plant Board
SECURITY BREACH POLICY
AND BREACH INVESTIGATION PLAN

SECTION 1. Purpose

The Kentucky General Assembly has established requirements for Kentucky public agencies regarding personal information security and breach investigations in KRS 61.931 to 61.934 (the Act). The Murray Electric Plant Board, which does business as Murray Electric System (MES) is adopting this Policy and Plan in compliance with the Act and in order to safeguard protected information. The purpose of this Policy is to inform employees and agents of MES and nonaffiliated third parties of MES's requirements and their responsibility for protecting personal or confidential records and information pursuant to the Act and to establish a response plan in the event that there is a breach of the security of records or information covered by the Act.

SECTION 2. Definitions

"Encryption" means the conversion of data using technology that:

1. Meets or exceeds the level adopted by the National Institute of Standards Technology as part of the Federal Information Processing Standards; and
2. Renders the data indecipherable without the associated cryptographic key to decipher the data.

"Nonaffiliated third party" means any person that:

1. Has a contract or agreement with MES; and
2. Receives personal information from MES pursuant to the contract or agreement.

"Personal Information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

1. Social Security Number;
2. Account number, credit card number, or debit card number that, in combination with any required security code, access code, or password will permit access to an account;
3. Tax payer identification number that incorporates a Social Security Number;
4. Driver's license, State identification card, or other identification number issued by a U.S. state or federal agency, e.g. Passport number; and
5. Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec 1232g.

"Public record or record" as established by KRS 171.410, means:

1. All books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings, and other documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of, or retained by a public agency.
2. "Public record" does not include any records owned by a private person or corporation that are not related to functions, activities, programs, or operations funded by state or local authority.

"Reasonable security and breach investigation procedures and practices" means data security procedures and practices developed in good faith and set forth in a written security information policy.

"Security breach" means:

1. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises, or that MES or a nonaffiliated third party reasonably believes may compromise, the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals; or
2. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises, or that MES or a nonaffiliated third party reasonably believes may compromise, the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.

Security Incident – A breach of information can occur physically or virtually.

A breach is considered to have taken place if any personal or confidential information contained in any record is suspected to have been stolen, viewed, copied, or otherwise compromised by an unauthorized individual or if it is suspected that information has been lost and could be accessed by unauthorized persons. The breach includes all MES entrusted information, whether stored physically on MES premises, cloud storage, a nonaffiliated third party's or agent's location, etc.

Access and use of personal or confidential information by an employee or agent of MES, or a nonaffiliated third party with authorized access to MES data and/or facilities for a legitimate business purpose of MES, is not a security breach, unless the personal or confidential information is used for a purpose that is not a lawful business purpose of MES or is used in a way that exposes the information to unauthorized disclosure.

Access and use of personal or confidential information disclosed to a federal, state, or local governmental entity for the performance of any statutory duty or responsibility is not considered a security breach.

Release of personal information about an individual who has consented in writing to its release to an identified third party is not considered a security breach.

SECTION 3. Responsibilities of MES Departments

3.1 Each department will develop and maintain standard procedures to provide staff with specific guidance on the protection of personal and confidential information used by or accessible to the department. Departmental procedures may supplement, but will not supersede, this Policy or applicable laws.

3.2 Each department shall ensure that vendors and service providers who may have access to personal or confidential information are aware of this Policy and MES's security requirements and breach procedures, and that these obligations are included in any contract or agreement with MES. Nonaffiliated third parties are required to meet or exceed the security requirements outlined in this Policy.

3.3 Department managers are responsible for determining which employees, agents, or nonaffiliated third parties are authorized to access and handle personal or confidential information and the department manager must ensure that the authorized individuals are adequately trained to handle such information and records in accordance with this Policy.

3.4 All employees who manage, access, or work with personal or confidential information or records shall read and sign MES's Employee Acknowledgement of MES Security Breach Policy and Breach Investigation Plan and Agreement annually. Each signed agreement shall be maintained in an MES file.

3.5 Department managers shall require all agents and nonaffiliated third parties who manage, access, or use personal or confidential information or records to read and sign MES's Nonaffiliated Party Acknowledgement of MES Security Breach Policy and Breach Investigation Plan and Agreement as part of the Terms and Conditions of doing business with MES. Each signed agreement shall be maintained in an MES file.

SECTION 4. Managing, maintaining, and storing personal and confidential information

4.1 Employees, agents, and nonaffiliated third parties who manage, access, or work with MES personal or confidential information are required to create, handle, maintain, and dispose of such information or records with prudent care in order to ensure their proper security. Personal or confidential information shall only be accessed and used by authorized employees, agents, and nonaffiliated third parties of MES for the purpose of performing services for MES.

4.2 The following procedures are to be followed while creating, handling, maintaining, storing, and disposing of records containing personal or confidential information.

1. Enter such information directly to a final authorized destination (i.e. computer system) and refrain from documenting the information elsewhere.
2. If such information is written on paper for reference, shred the paper within a period as set in our Company retention policy and saving the information in its final destination.
3. Electronic payment data should only be handled by authorized personnel.

4. Such information should not be included on e-mails, unless other means of transmittal of the information are impractical and the information is marked "confidential."
5. Such information should not be included on printed reports except as needed for the performance of essential tasks.
6. Maintain records that contain such information in a secured room and limit access to the area.
7. If possible, utilize encryption to secure such information in the database or storage system.
8. Do not leave a computer unattended if such information could be accessed by unauthorized individuals.
9. Do not store files with such information on laptops or on portable drives, e.g. thumb drives, unless the records or information and the device can be secured and not accessible by unauthorized individuals.
10. Take reasonable measures when destroying such information, records, or data that is eligible for disposal to prevent the information from being read or reconstructed. Documents containing such information or data should be shredded by or under the supervision of an individual who has authorized access to the data. A third party may be employed by MES to destroy such information in a manner consistent with this Policy, upon written approval by a department manager.

4.3 Personal or confidential information shall only be released to the account holder or to an individual to whom the information relates, after adequate confirmation of personal identifying information or the presentation of a valid picture ID. The confirmed account holder or individual must authorize the release of sensitive information to any third party. Confidential information will only be released in accordance with applicable law. Records may be released pursuant to a court order, warrant, subpoena, or other legal process.

SECTION 5. Security Breach or Identity Theft

5.1 MES shall attempt to identify security breaches and potential threats of identity theft. Each department shall establish indicators to help in the detection of security breaches and identity theft and unauthorized use of personal information.

5.2 Indicia shall include, but not be limited to:

1. An employee, vendor, or customer provides notice that he or she is a victim of identity theft.
2. A consumer reporting agency or service provider provides an alert, notification, or other warning.
3. Records appear to have been altered or forged.
4. Personal identifying information provided to MES is not consistent with other available information sources, e.g. information presented is inconsistent with other records within MES.
5. Notice from a law enforcement officer or other credible person that an MES account/record has been fraudulently opened, accessed, or used by an unauthorized person who may be engaged in identity theft or other illegal or unauthorized activity.

5.3 Upon identification of a security breach or a potential risk of identity theft, an employee shall immediately notify his or her immediate supervisor in person or by telephone to determine the appropriate course of action in accordance with this Policy. MES supervisors shall immediately notify the department manager who is responsible for further investigation and notification. If the breach

involves electronic equipment, the MES Help Desk shall be notified by telephone or in person as soon as possible.

An agent of MES or nonaffiliated third party who determines that there has been a security breach of personal information shall notify MES's Chief Network Administrator and MES's Broadband Customer Service Manager as soon as possible, but within seventy-two (72) hours of such determination. The notice shall include all known information about the security breach at the time of the notification. The notice shall only be delayed if a law enforcement agency notifies the agent or nonaffiliated third party that notice will impede a criminal investigation or jeopardize homeland or national security.

Broadband Customer Service Manager and Privacy Officer, Tina Cox – 270-762-1719
Chief Network Administrator, Chad Lawson – 270-762-1722
If unable to reach either MES contact, call 270-753-5312 and ask to speak to the General Manager about the incident.

Notice of a potential security breach related to personal or confidential information must be given as soon as possible, but within 72 hours of a determination that a breach has occurred to the following agencies, utilizing the form, if any, provided by the Commonwealth Office of Technology:

a. Commissioner of the Kentucky State Police
   KSP Headquarters
   919 Versailles Road
   Frankfort, KY 40601
   502-782-1800
   www.kentuckystatepolice.org
b. Auditor of Public Accounts
   209 St. Clair Street
   Frankfort, KY 40601
   502-564-5841
   http://auditor.ky.gov
c. Attorney General
   Office of the Attorney General
   700 Capitol Avenue, Suite 118
   Frankfort, KY 40601-3449
   502-696-5300
   http://ag.ky.gov
d. Commissioner of the Department for Local Government
   1024 Capital Center Drive, Suite 340
   Frankfort, KY 40601
   502-573-2382
   https://kydlgweb.ky.gov

SECTION 6. Incident Response Plan

6.1 Step 1. Investigate the security breach that is believed to have occurred.

Physical Breach - The following are indications that there has been unauthorized access to personal or confidential information through a physical breach:

a. Evidence of lock tampering on file cabinets or office doors.
b. Evidence of unauthorized entry in an area where personal or confidential information is stored.
c. Missing files or records that contain personal or confidential information.
d. Any other circumstances that indicate that a physical breach of security has occurred.

Technology Breach - The following are indications that there has been unauthorized access to personal or confidential information through a technology breach.

a. An unknown or unauthorized name appears in the computer logon window.
b. Disconnected computer cables or power cables.
c. Missing computer equipment (desktop, laptop, tablet, etc.).
d. Evidence that electronic files or records have been accessed by unknown or unauthorized individuals, or are missing.
e. Any devices or media are found attached to the computer that are not known or authorized.
f. Unusual programs, icons, or windows appear that are not recognized or are not part of the normal work process.
g. Any other suspicious activity or circumstances which indicate an attempt to use technology or records without authorization.

Step 2. Notification to Agencies – Upon conclusion of the investigation, if MES determines that a security breach has occurred and that the misuse of personal information has occurred or is reasonably likely to occur, MES shall notify the following agencies within 48 hours of confirming an actual security breach (this is in addition to the initial contact required during the first 72 hours):

a. Commissioner of the Kentucky State Police
   KSP Headquarters
   919 Versailles Road
   Frankfort, KY 40601
   502-782-1800
   www.kentuckystatepolice.org
b. Auditor of Public Accounts
   209 St. Clair Street
   Frankfort, KY 40601
   502-564-5841
   http://auditor.ky.gov
c. Attorney General
   Office of the Attorney General

700 Capitol Avenue, Suite 118
Frankfort, KY 40601-3449
502-696-5300
http://ag.ky.gov

d. Commissioner of the Department for Local Government
1024 Capital Center Drive, Suite 340
Frankfort, KY 40601
502-573-2382
https://kydlgweb.ky.gov

Step 3. Investigation and remediation of the breach.

MES will designate an Incident Response Team to investigate and handle the security breach until such time that the threat has ended and affected individuals and agencies have been notified. This may include, but shall not be limited to:

e. Implementing additional technology monitoring.
f. Upgrading / modifying technology security.
g. Repairing / replacing breaches, e.g. door locks.
h. Additional security incident policy training.

Step 4. Post-investigation notification.

Internal notification – Employees, agents, and nonaffiliated third parties who were included in the identification and investigation of a suspected or actual security breach will be notified of the result upon completion of the remediation.

Determination regarding notice - If MES's investigation determines that the misuse of personal information has not occurred and is not likely to occur, MES is not required to give notice to impacted persons, but MES shall maintain records that reflect the basis for its decision for a retention period set by the State Archives and Records Commission as established by KRS 171.420. MES shall notify the appropriate entities listed in Step 2 of this subsection, paragraph 6.1, that the misuse of personal information has not occurred.

Notice to impacted persons. If the investigation determines that misuse of personal information has occurred or is reasonably likely to occur, MES shall complete the following actions within thirty-five (35) days of known security breaches. Notice shall be provided to individuals impacted by the breach. Notice may be delayed if law enforcement informs MES that disclosure of the breach will impede a criminal investigation or jeopardize national security. Such request by law enforcement must be documented in writing. Delay of notification shall be documented in writing on a form provided by the Commonwealth Office of Technology.

Notices shall provide, at a minimum:

i. A general description of the breach, the type of personal or confidential information that was breached, and the actions that MES has taken to protect the information from further

access.

j. MES's local number so that persons may call for further information and assistance.
k. MES's physical address so that persons may visit to request further information and assistance.
l. Toll-free numbers, addresses, and web site addresses for major consumer credit agencies.
m. Toll-free number, address, and web site address for the Federal Trade Commission.
n. Toll-free number, address, and web site address for the Office of the Kentucky Attorney General.
o. A notice to alert credit agencies of potential fraud or identity theft and to remain vigilant by reviewing account statements and monitoring free credit reports.

If a security breach involves more than 1,000 persons, notification shall include:

a. Written notice of the timing, distribution, and content of the notice to the Commonwealth Office of Technology, Department of Local Government, as well as to all consumer reporting agencies that are included on the list maintained by the Office of the Attorney General, that compile and maintain files on consumers on a nationwide basis. This action shall be completed at least seven (7) days prior to providing any notifications below.
b. Conspicuous posting of the notice on the MES.org web site.
c. Regional or local media, if the security breach is localized. Notification to major statewide media, if the security breach is widespread, including broadcast media such as radio and television.
d. Affected individuals via:
    i. Written notice;
    ii. Electronic notice to those individuals for whom MES has a valid email address and who have agreed to receive electronic communications; and
    iii. Telephone notice, provided the contact is made directly with the affected persons and appropriately documented by MES.

Step 5. Post-incident measures – Document the event, including the collection and filing of relevant information and records in a sterile and secure location. Hold a "lessons learned" session with all breach response team members who were involved in each response so that the process may be improved.

At least annually, MES's Incident Response Oversight Team will review all incidents of potential or actual security breaches and report findings and recommendations to the General Manager.

SECTION 7. Acknowledgements and Agreements

7.1 All employees who collect, maintain, store, or use personal information shall execute an acknowledgement and agreement in substantially the form attached hereto as Exhibit 1.

7.2 All nonaffiliated third parties to whom personal information is disclosed by MES shall execute an acknowledgement and agreement in substantially in the form attached hereto as Exhibit 2, or execute an agreement with MES containing terms required by the Act.

Murray Electric Plant Board
EMPLOYEE ACKNOWLEDGMENT OF MES SECURITY BREACH POLICY AND
BREACH INVESTIGATION PLAN AND AGREEMENT

I have read the MES Security Breach Policy and Breach Investigation Plan of Murray Electric Plant Board (MES) and understand how to properly manage, maintain, store, and dispose of personal and confidential MES information. I agree to abide by the Policy and will handle personal and confidential information with prudent care in order to ensure proper security of the information and records.

In the event of a suspected or actual breach of personal or confidential information, I will notify my immediate supervisor, via telephone or in person, without delay and follow the Incident Response Plan.

I understand that failure to comply with the Policy, or negligent handling or inappropriate use of MES's personal or confidential information may subject me to disciplinary action up to and including dismissal from my employment.

I have read, understand, and agree to the above.

Printed Name: _____

Department: _____

Signature: _____

Date Signed: _____

Exhibit 1

Murray Electric Plant Board
NONAFFILIATED PARTY ACKNOWLEDGMENT OF MES SECURITY BREACH POLICY AND BREACH INVESTIGATION PLAN AND AGREEMENT

I have read the MES Security Breach Policy and Breach Investigation Plan of Murray Electric Plant Board (MES) and understand how MES manages, maintains, stores, and disposes of personal and confidential MES information. I represent and agree that my company/entity has security procedures or practices to protect personal and confidential information maintained by or received from MES and that my company/entity will maintain and update procedures and practices to protect and safeguard such information against security breaches and that its security measures and breach investigation plan will be at least as stringent as the requirements of KRS 61.931, et seq.

In the event of a suspected or actual breach of personal or confidential information, we will notify the following MES employees, without delay: MES' Broadband Customer Service Manager and Privacy Officer, Tina Cox at 270-762-1719 and MES's Chief Network Administrator, Chad Lawson, at 270-762-1722. If unable to reach either MES contact, I will call 270-753-5312 and ask to speak to the General Manager about the incident.

I represent that I am authorized to execute this acknowledgment and agreement on behalf of the company/entity identified below which shall be responsible for any actions of any individuals within the entity related to this Policy.

I understand that breach of the Policy or plan, or this agreement, may result in termination of services of my entity, without penalty.

I have read, understand, and agree to the above.

Printed Name: _____

Entity/Company: _____

Signature: _____

Date Signed: _____

Exhibit 2