



Filing Receipt

Received - 2022-04-18 03:56:40 PM
Control Number - 53385
ItemNumber - 421



**Golden Spread Electric Cooperative, Inc.
("GSEC")
Emergency Operations Plan
Executive Summary
Pursuant to 16 Texas Administrative
Code ("TAC") § 25.53**

April 2022

**GSEC Emergency Operations
Plan (“EOP”) Executive Summary
Pursuant to 16 TAC § 25.53**

Table of Contents

List of Acronyms	3
1. Introduction and Applicability	4
2. Contents and Policies	4
3. 16 TAC §25.53 Reference Table	6
4. Record of Distribution	14
5. Emergency Contacts	16
Affidavit	17

List of Acronyms

AEEC	Antelope Elk Energy Center
EOP	Emergency Operations Plan
ERCOT	Electric Reliability Council of Texas, Inc.
GSEC	Golden Spread Electric Cooperative, Inc.
GSPWR	Golden Spread Panhandle Wind Ranch, LLC
REP	Retail Electric Provider
TAC	Texas Administrative Code

GSEC EOP Executive Summary Pursuant to 16 TAC § 25.53

1. Introduction and Applicability

This EOP Executive Summary is submitted by GSEC in accordance with 16 TAC § 25.53. GSEC is an electric cooperative with both generation and transmission facilities, therefore it responds to all components of 16 TAC § 25.53(d) with the exception of rules applicable to retail electric providers ("REPs") and Electric Reliability Council of Texas ("ERCOT"), and files annexes to its EOP as applicable in accordance with those required by 16 TAC § 25.53(e)(1) and 16 TAC § 25.53(e)(2).

2. Contents and Policies

Table 1 below provides an overview of the contents and policies contained in GSEC's EOP, as well as the sections of the EOP in which they can be located.

Table 1. Overview of Contents and Policies Included in GSEC's EOP

EOP Section(s)	Title	Description
1-1.5	Approval and Implementation	These sections contain an introduction to GSEC's EOP, an overview of GSEC and its operations, the individuals responsible for components of the GSEC EOP, a revision control summary, and GSEC's statement on approval.
2-2.3	Communication Plan	These sections describe the communication procedures GSEC utilizes for both its generation and transmission facilities during an emergency situation.
3	Pre-Identified Supplies Plan	This section describes GSEC's plan to maintain pre-identified supplies for emergency response.
4	Emergency Staffing Plan	This section describes how GSEC addresses staffing its facilities during an emergency response.
5	Severe-Weather Identification Plan	This section addresses how GSEC identifies weather-related hazards, and the process GSEC follows to activate its EOP.
6.1-6.1.2.8	Transmission Facility Annexes	These sections identify the transmission facilities GSEC owns, including those operated by Special Facility Agreement by member cooperatives and the GSEC Operations Center, and includes the annexes required by 16 TAC § 25.53(e)(1), as applicable.

EOP Section(s)	Title	Description
6.2-6.2.3.7	Generating Facility Annexes	These sections identify the generating facilities GSEC owns and includes the annexes required by 16 TAC § 25.53(e)(2), as applicable. These sections are broken down by the three GSEC generating facilities; Mustang Station, Antelope Elk Energy Center ("AEEC"), and Golden Spread Panhandle Wind Ranch, owned by GSEC's wholly owned subsidiary, Golden Spread Panhandle Wind Ranch, LLC ("GSPWR").
7	Drills	This section addresses the 16 TAC § 25.53(f) requirement for GSEC to conduct an annual drill testing its EOP.
8	Reporting Requirements	This section addresses the 16 TAC § 25.53(g) requirement for GSEC to report to PUCT upon request and in emergency events.
9	Copy Available for Inspection	This section addresses the 16 TAC § 25.53(c)(1)(D) requirement for GSEC to provide an unredacted copy of its EOP to commission staff upon request by commission staff.
Appendix A	Pandemic Preparedness Plan	This appendix includes GSEC's plan for preparing for and responding to pandemics and epidemics.
Appendix B	Cyber Security Plan	This appendix includes GSEC's Incident Reporting and Response Plan which addresses how GSEC handles cyber security incidents.
Appendix C	Physical Security Incident Plan	This appendix includes GSEC's Emergency Action Plan which includes GSEC procedures for handling instances of physical security incidents.
Appendix D	Mustang Station Procedures	This appendix includes the plant specific emergency operating procedures and plans for GSEC's generating facility, Mustang Station.
Appendix E	AEEC Procedures	This appendix includes the plant specific emergency operating procedures and plans for GSEC's generating facility, AEEC.
Appendix F	GSPWR Procedures	This appendix includes the plant specific emergency operating procedures and plans for GSEC's generating facility, GSPWR.
Appendix G	GSEC Operations Center Procedures	This appendix includes the site specific emergency operating procedures and plans for GSEC's transmission facility, GSEC Operations Center.

3. 16 TAC § 25.53 Reference Table

The table below contains the cross-references to specific sections and page numbers of GSEC's Emergency Operations Plan that correspond with the requirements of 16 TAC § 25.53 pursuant to 16 TAC § 25.53(c)(1)(A)(i)(II).

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
1	16 TAC § 25.53(c)(4)(A)(i)-(ii)	An entity must file a record of distribution that contains the following information in table format: (i) titles and names of persons in the entity's organization receiving access to or training on the EOP; and (ii) dates of access to or training on the EOP, as appropriate.	Yes	Executive Summary, Section 4	14-15
2	16 TAC § 25.53(c)(4)(B)	A list of primary and, if possible, backup emergency contacts for the entity, including identification of specific individuals who can immediately address urgent requests and questions from the commission during an emergency.	Yes	Executive Summary, Section 5	16
3	16 TAC § 25.53(c)(4)(C)(i)-(vi)	An affidavit from the entity's highest-ranking representative, official, or officer with binding authority over the entity affirming the following: (i) relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP, and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency; (ii) the EOP has been reviewed and approved by the appropriate executives; (iii) drills have been conducted to the extent required by subsection (f) of this section; (iv) the EOP or an appropriate summary has been distributed to local jurisdictions as needed; (v) the entity maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and (vi) the entity's emergency management personnel who are designated to interact with local, state, and federal	Yes	Executive Summary	17

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
		emergency management officials during emergency events have received the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training.			
4	16 TAC § 25.53(d)(1)(A)	An approval and implementation section that: (A) introduces the EOP and outlines its applicability;	Yes	EOP, Sections 1.1, 1.2	4-5
5	16 TAC § 25.53(d)(1)(B)	An approval and implementation section that: (B) lists the individuals responsible for maintaining and implementing the EOP, and those who can change the EOP;	Yes	EOP, Section 1.3	5-6
6	16 TAC § 25.53(d)(1)(C)	An approval and implementation section that: (C) provides a revision control summary that lists the dates of each change made to the EOP since the initial EOP filing pursuant to paragraph (c)(1) of this section;	Yes	EOP, Section 1.4	6
7	16 TAC § 25.53(d)(1)(D)	An approval and implementation section that: (D) provides a dated statement that the current EOP supersedes previous EOPs;	Yes	EOP, Section 1.5	7
8	16 TAC § 25.53(d)(1)(E)	An approval and implementation section that: (E) states the date the EOP was most recently approved by the entity.	Yes	EOP, Section 1.5	7
9	16 TAC § 25.53(d)(2)(A)	A communication plan (A) An entity with transmission or distribution service operations must describe the procedures during an emergency for handling complaints and for communicating with the public; the media; customers; the commission; the Office of the Public Utility Counsel ("OPUC"); local and state governmental entities, officials, and emergency operations centers, as appropriate in the circumstances for the entity; the reliability coordinator for its power region; and critical load customers directly served by entity.	Yes	EOP, Sections 2.1, 2.2	6-7

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
10	16 TAC § 25.53(d)(2)(B)	A communication plan (B) An entity with generation operations must describe the procedures during an emergency for communicating with the media; the commission; OPUC; fuel suppliers; local and state governmental entities, officials, and emergency operations centers, as appropriate in the circumstances for the entity; and the applicable reliability coordinator.	Yes	EOP, Sections 2.1, 2.3	6-7
11	16 TAC § 25.53(d)(3)	A plan to maintain pre-identified supplies for emergency response.	Yes	EOP, Section 3	7-8
12	16 TAC § 25.53(d)(4)	A plan that addresses staffing during emergency response.	Yes	EOP, Section 4	8
13	16 TAC § 25.53(d)(5)	A plan that addresses how an entity identifies weather-related hazards, including tornadoes, hurricanes, extreme cold weather, extreme hot weather, drought, and flooding, and the process the entity follows to activate the EOP.	Yes	EOP, Section 5	8
Annexes Required by 16 TAC § 25.53(e)(1) – Transmission Facilities					
14	16 TAC § 25.53(e)(1)(A)(i)	An electric utility, a transmission and distribution utility a municipally owned utility, and an electric cooperative must include in its EOP for its transmission and distribution facilities the following annexes: (A) a weather emergency annex that includes: (i) operational plans for responding to a cold or hot weather emergency, distinct from the weather preparations required under §25.55 of this title (relating to Weather Emergency Preparedness);	Yes	EOP, Sections 6.1.1, 6.1.2.1	8-9
15	16 TAC § 25.53(e)(1)(A)(ii)	An electric utility, a transmission and distribution utility a municipally owned utility, and an electric cooperative must include in its EOP for its transmission and distribution facilities the following annexes: (A) a weather emergency annex that includes: (ii) a checklist for	Yes	EOP, Sections 6.1.1, 6.1.2.1	8-9

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
		transmission or distribution facility personnel to use during cold or hot weather emergency response that includes lessons learned from past weather emergencies to ensure necessary supplies and personnel are available through the weather emergency.			
16	16 TAC § 25.53(e)(1)(B)(i)	A load shed annex that must include: (i) procedures for controlled shedding of load;	Yes	EOP, Sections 6.1.1, 6.1.2.2, 6.1.2.2.1, Appendix G	8-9, 579
17	16 TAC § 25.53(e)(1)(B)(ii)	A load shed annex that must include: (ii) priorities for restoring shed load to service;	Yes	EOP, Sections 6.1.1, 6.1.2.2, 6.1.2.2.2, Appendix G	8-10, 579
18	16 TAC § 25.53(e)(1)(B)(iii)	A load shed annex that must include: (iii) a procedure for maintaining an accurate registry of critical load customers, as defined under 16 TAC § 25.5(22) of this title (relating to Definitions), § 25.52(c)(1) and (2) of this title (relating to Reliability and Continuity of Service) and § 25.497 of this title (relating to Critical Load Industrial Customers, Critical Load Public Safety Customers, Critical Care Residential Customers, and Chronic Condition Residential Customers), and TWC § 13.1396 (relating to Coordination of Emergency Operations), directly served, if maintained by the entity. The registry must be updated as necessary but, at a minimum, annually. The procedure must include the processes for providing assistance to critical load customers in the event of an unplanned outage, for communicating with critical load customers during an emergency, coordinating with government and service agencies as necessary during an emergency, and for training staff with respect to serving critical load customers.	No	EOP, Section 6.1.2.2.3	10

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
19	16 TAC § 25.53(e)(1)(C)	A pandemic and epidemic annex	Yes	EOP, Sections 6.1.1, 6.1.2.3, Appendix A	8, 10, 16
20	16 TAC § 25.53(e)(1)(D)	A wildfire annex	No	EOP, Sections 6.1.1, 6.1.2.4	8, 10
21	16 TAC § 25.53(e)(1)(E)	A hurricane annex that includes evacuation and re-entry procedures if facilities are located within a hurricane evacuation zone, as defined by the Texas Division of Emergency Management (TDEM)	No	EOP, Sections 6.1.1, 6.1.2.5	8, 10
22	16 TAC § 25.53(e)(1)(F)	A cyber security annex	Yes	EOP, Sections 6.1.1, 6.1.2.6, Appendix B	8, 11, 24
23	16 TAC § 25.53(e)(1)(G)	A physical security incident annex	Yes	EOP, Sections 6.1.1, 6.1.2.7, Appendix C	8, 11, 42
24	16 TAC § 25.53(e)(1)(H)	A transmission and distribution utility that leases or operates facilities under PURA § 39.918(b)(1) or procures, owns, and operates facilities under PURA § 39.918(b)(2) must include an annex that details its plan for the use of those facilities	No	EOP, Sections 6.1.1, 6.1.2.8	8, 11
Annexes Required by 16 TAC § 25.53(e)(2) – Generating Facilities					
25	16 TAC § 25.53(e)(2)(A)(i)	An electric cooperative, an electric utility, or a municipally owned utility that operate a generation resource in Texas; and a PGC must include the following annexes for its generation resources other than generation resources authorized under PURA § 39.918: (A) a weather emergency annex that includes (i) operational plans for responding to a cold or hot weather emergency, distinct from the weather preparations required under § 25.55 of this title;	Yes	EOP, Sections 6.2.1.1.1, 6.2.2.1.1, 6.2.3.1.1, Appendix D, Appendix E, Appendix F	11, 13, 14, 56, 205, 500
26	16 TAC § 25.53(e)(2)(A)(ii)	An electric cooperative, an electric utility, or a municipally owned utility that operate a generation resource in Texas;	Yes	EOP, Sections 6.2.1.1.2, 6.2.2.1.2,	11, 13, 14, 56,

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
		and a PGC must include the following annexes for its generation resources other than generation resources authorized under PURA § 39.918: (A) a weather emergency annex that includes (ii) verification of the adequacy and operability of fuel switching equipment, if installed;		6.2.3.1.2, Appendix D, Appendix E, Appendix F	205, 500
27	16 TAC § 25.53(e)(2)(A)(iii)	An electric cooperative, an electric utility, or a municipally owned utility that operate a generation resource in Texas; and a PGC must include the following annexes for its generation resources other than generation resources authorized under PURA § 39.918: (A) a weather emergency annex that includes (iii) a checklist for generation resource personnel to use during a cold or hot weather emergency response that includes lessons learned from past weather emergencies to ensure necessary supplies and personnel are available through the weather emergency.	Yes	EOP, Sections 6.2.1.1.3, 6.2.2.1.3, 6.2.3.1.3, Appendix D, Appendix E, Appendix F	11-12, 13, 14, 56, 205, 500
28	16 TAC § 25.53(e)(2)(B)	A water shortage annex that addresses supply shortages of water used in the generation of electricity;	Yes	EOP, Sections 6.2.1.2, 6.2.2.2, 6.2.3.2, Appendix D, Appendix E	12, 13, 14, 56, 205
29	16 TAC § 25.53(e)(2)(C)	A restoration of service annex that identifies plans intended to restore to service a generation resource that failed to start or that tripped offline due to a hazard or threat	Yes	EOP, Sections 6.2.1.6, 6.2.2.3, 6.2.3.3, Appendix D, Appendix E, Appendix F	12, 13, 14, 56, 205, 500
30	16 TAC § 25.53(e)(2)(D)	A pandemic and epidemic annex	Yes	EOP, Sections 6.2.1.3, 6.2.2.4, 6.2.3.4 Appendix A	12, 13, 15, 16

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
31	16 TAC § 25.53(e)(2)(E)	A hurricane annex that includes evacuation and re-entry procedures if facilities are located within a hurricane evacuation zone, as defined by TDEM.	No	EOP, Sections 6.2.1.4, 6.2.2.5, 6.2.3.5	12, 13, 15
32	16 TAC § 25.53(e)(2)(F)	A cyber security annex	Yes	EOP, Sections 6.2.1.5, 6.2.2.6, 6.2.3.6, Appendix B	12, 14, 15, 24
33	16 TAC § 25.53(e)(2)(G)	A physical security incident annex	Yes	EOP, Sections 6.2.1.7, 6.2.2.7, 6.2.3.7, Appendix C	12, 14, 15, 42
34	16 TAC § 25.53(f)	An entity must conduct or participate in at least one drill each calendar year to test its EOP. Following an annual drill the entity must assess the effectiveness of its emergency response and revise its EOP as needed. If the entity operates in a hurricane evacuation zone as defined by TDEM, at least one of the annual drills must include a test of its hurricane annex. An entity conducting an annual drill must, at least 30 days prior to the date of at least one drill each calendar year, notify commission staff, using the method and form prescribed by commission staff on the commission's website, and the appropriate TDEM District Coordinators, by email or other written form, of the date, time, and location of the drill. An entity that has activated its EOP in response to an emergency is not required under this subsection to conduct or participate in a drill in the calendar year in which the EOP was activated.	Yes	EOP, Section 7	15

Line No.	Rule Reference	Rule Description	Applicable to GSEC	Document/Section(s)	Page(s)
35	16 TAC § 25.53(g)	Upon request by commission staff during an activation of the State Operations Center by TDEM, an affected entity must provide updates on the status of operations, outages, and restoration efforts. Updates must continue until all incident-related outages of customers able to take service are restored or unless otherwise notified by commission staff. After an emergency, commission staff may require affected entity to provide an after action or lessons learned report and file it with the commission by a date specified by staff.	Yes	EOP, Section 8	15

4. Record of Distribution

The table below contains the record of employee distribution for GSEC's Emergency Operations Plan pursuant to 16 TAC § 25.53(c)(4)(A)(i)-(ii).

Line No.	Name	Title	Last Date of Distribution	Last Date of Training
1	Beard, Mark	System Operator II	4/18/2022	N/A
2	Berry, Maggie	Associate General Counsel	4/18/2022	N/A
3	Boatler, Tyson	Manager of Trading	4/18/2022	N/A
4	Boatright, Ty	Senior Production Asset Manager	4/18/2022	N/A
5	Calderon, Ruth	Environmental Policy & Legislative Affairs Manager	4/18/2022	N/A
6	Cross, Steve	Director, Power Supply	4/18/2022	N/A
7	Diaz, Lacy	Human Resources Director	4/18/2022	N/A
8	Dye, David	System Operator II	4/18/2022	N/A
9	Eichelmann, John	VP, Member Services and Power Delivery	4/18/2022	N/A
10	Gauna, Alicia	Information Security Manager	4/18/2022	N/A
11	Goddard, Tony	System Operator II	4/18/2022	N/A
12	Guy, James	General Counsel, Chief Legal & Compliance Officer	4/18/2022	N/A
13	Hale, Laura	Senior Counsel	4/18/2022	N/A
14	Hedtke, Jon	Manager, End User Computer & IT Member Services	4/18/2022	N/A
15	Henderson, Natasha	Director, Compliance, Market and Regulatory Affairs	4/18/2022	N/A
16	Hollandsworth, Kari	President and Chief Executive Officer	4/18/2022	N/A
17	Johnson, Doug	Insurance & Contract Manager	4/18/2022	N/A
18	Johnson, Will	Manager of SCADA Services	4/18/2022	N/A
19	Lambrano, Johnathan	System Operator II	4/18/2022	N/A
20	Lancaster, Larami	HR Generalist	4/18/2022	N/A
21	Lester, Wallace	Safety & Project Coordinator	4/18/2022	N/A
22	Lowe, Matt	Chief Financial Officer	4/18/2022	N/A
23	Marsh, Dave	Senior Production Asset Manager	4/18/2022	N/A
24	McMinn, Shane	Director, Power Delivery	4/18/2022	N/A
25	Moore, Matt	VP, Commercial & Asset Operations	4/18/2022	N/A
26	Orr, Sara	Compliance Engineer	4/18/2022	N/A
27	Perez, Anthony	Senior Project Manager	4/18/2022	N/A

Line No.	Name	Title	Last Date of Distribution	Last Date of Training
28	Price, Jett	Manager of Enterprise Risk	4/18/2022	N/A
29	Stephens, Andy	Operations Center Manager	4/18/2022	N/A
30	Stewart, Roxann	Senior Payroll & Compliance Specialist	4/18/2022	N/A
31	Stollings, Nathan	Senior Network Administrator	4/18/2022	N/A
32	Usleton, Sean	Executive IT Director	4/18/2022	N/A
33	Vigil, Dillan	Compliance Engineer	4/18/2022	N/A
34	Warren, Robert	System Operator II	4/18/2022	N/A
35	Webb, Cody	Director of Infrastructure & Information Security	4/18/2022	N/A
36	Wells, Stephanie	Compliance Analyst	4/18/2022	N/A
37	Whitworth, William	Production Compliance Analyst	4/18/2022	N/A
38	Wiegand, Steve	Manager Treasury & Finance	4/18/2022	N/A
39	Wise, Mike	SVP, Regulatory & Market Strategy	4/18/2022	N/A
40	Yeary, Bret	Manager of Plant Performance and Projects	4/18/2022	N/A

5. Emergency Contacts

The table below contains the list of emergency contacts for GSEC. pursuant to 16 TAC § 25.53(c)(4)(B). These are the contacts who can immediately address urgent requests and questions from the commission during an emergency.

Designation	Name	Title	Phone	E-mail
Primary	Stephen Cross	Director, Power Supply	[REDACTED]	[REDACTED]
Primary	Shane McMinn	Director, Power Delivery	[REDACTED]	[REDACTED]
Back-Up	Kari Hollandsworth	President and Chief Executive Officer	[REDACTED]	[REDACTED]
Back-Up	Matthew C. Moore	VP, Commercial and Asset Operations	[REDACTED]	[REDACTED]
Back-Up	John Eichelmann	VP, Member Services and Power Delivery	[REDACTED]	[REDACTED]

Affidavit

STATE OF TEXAS §

COUNTY OF POTTER §

BEFORE ME, the undersigned authority, on this day personally appeared, and who, after being duly sworn, stated on his or her oath that he or she is entitled to make this Affidavit, and that the statements contained below are based on personal knowledge and are true and correct.

I, Kari Hollandsworth, swear or affirm the following on behalf of Golden Spread Electric Cooperative, Inc., an electric cooperative operating in the State of Texas:

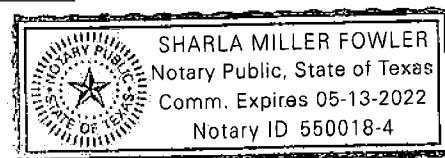
- a. In accordance with 16 TAC § 25.53(c)(4)(C)(i), all relevant operating personnel identified in the Record of Distribution table in Section 4 of the Executive Summary are familiar with and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency. In accordance with guidance received during the March 11, 2022 PUCT workshop, such personnel have not yet received training on the EOP; however, training will be provided no later than December 31, 2022;
- b. The EOP has been reviewed and approved by the appropriate executives identified in Attachment A to this affidavit;
- c. In accordance with the guidance received during the March 11, 2022 PUCT workshop, Golden Spread Electric Cooperative, Inc. is providing the Commission with its schedule for complying with 16 TAC § 25.53(f) related to annual drills. One or more drills are tentatively planned for completion by Fall 2022;
- d. Golden Spread Electric Cooperative, Inc. determined that there was not a need to distribute to local jurisdictions at this time;
- e. Golden Spread Electric Cooperative, Inc. maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and
- f. Golden Spread Electric Cooperative, Inc.'s emergency management personnel, identified in Attachment B, who are designated to interact with local, state, and federal emergency management officials during emergency events have received the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training.

Kari Hollandsworth
Kari Hollandsworth, President & CEO
Golden Spread Electric Cooperative, Inc.


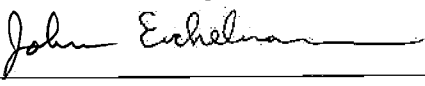
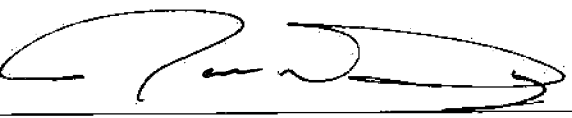
Sworn to and subscribed before me on this 18th day of April, 2022

Sharla Miller Fowler

Notary Public in and for the State of Texas Notary Seal

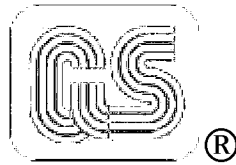


Attachment A to the Affidavit

Executive	Signature	Date
Matthew C. Moore VP, Commercial & Asset Operations		4/14/2022
John Eichelmann VP, Member Services and Power Delivery		4/14/2022
James E. Guy General Counsel, Chief Legal & Compliance Officer		4/14/2022

Attachment B to the Affidavit

Name	Title	Training Received	Training Completion
GSEC Operations Center Emergency Management Personnel			
Shane McMinn	Director of Power Delivery	IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training	3/28/2022
Andy Stephens	Operations Center Manager	IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training	3/9/2022
GSEC Generating Facilities Emergency Management Personnel			
David Marsh	Senior Production Asset Manager	IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training	3/30/2022
Ty Boatright	Senior Production Asset Manager	IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training	4/1/2022
GSEC Corporate Emergency Management Personnel			
Jett Price	Manager of Enterprise Risk	IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training	4/6/2022



**Golden Spread Electric Cooperative, Inc.
("GSEC")
Emergency Operations Plan
Pursuant to 16 Tex. Admin. Code
("TAC") § 25.53**

April 2022

**Golden Spread Electric
Cooperative, Inc. ("GSEC")
Emergency Operations Plan
Pursuant to
16 TAC § 25.53**

Table of Contents

TABLE OF APPENDICES	II
LIST OF ACRONYMS	III
1. APPROVAL AND IMPLEMENTATION	4
1.1 INTRODUCTION AND APPLICABILITY	4
1.2 GSEC OVERVIEW	4
1.3 EOP RESPONSIBILITIES	5
1.4 REVISION CONTROL SUMMARY	6
1.5 STATEMENT ON APPROVAL	6
2. COMMUNICATION PLAN	6
2.1 OVERVIEW	6
2.2 GSEC OPERATIONS CENTER COMMUNICATIONS PLAN	6
2.3 GENERATING FACILITIES COMMUNICATIONS PLAN	7
3. PRE-IDENTIFIED SUPPLIES PLAN	7
4. EMERGENCY STAFFING PLAN	8
5. SEVERE-WEATHER IDENTIFICATION PLAN	8
6. ANNEXES PURSUANT TO 16 TAC § 25.53(E)	8
6.1 TRANSMISSION FACILITY ANNEXES	8
6.1.1 <i>Transmission Facilities</i>	8
6.1.2 <i>GSEC Operations Center</i>	9
6.2 GENERATING FACILITY ANNEXES	11
6.2.1 <i>Mustang Station</i>	11
6.2.2 <i>AEEC</i>	12
6.2.3 <i>GSPWR</i>	14
7. DRILLS	15
8. REPORTING REQUIREMENTS	15
9. COPY AVAILABLE FOR INSPECTION	15
APPENDIX A	16
APPENDIX B	24
APPENDIX C	42
APPENDIX D	56
APPENDIX E	205
APPENDIX F	500
APPENDIX G	579

Table of Appendices

Appendix A	Pandemic Preparedness Plan
Appendix B	Cyber Security Annex
Appendix C	Physical Security Incident Annex
Appendix D	Mustang Station Procedures
Appendix E	Antelope Elk Energy Center Procedures
Appendix F	Golden Spread Panhandle Wind Ranch Procedures
Appendix G	GSEC Operations Center Procedures

List of Acronyms

ACES	Alliance for Cooperative Energy Services Power Marketing LLC
AEEC	Antelope Elk Energy Center
BA	Balancing Authority
ELCP	Emergency Load Curtailment Program
EOP	Emergency Operations Plan
ERCOT	Electric Reliability Council of Texas
GOP	Generator Operator
GSEC	Golden Spread Electric Cooperative, Inc.
GSPWR	Golden Spread Panhandle Wind Ranch
ICE	Intercontinental Exchange
LSE	Load Serving Entity
Member	A rural electric distribution cooperative and one of the 16 members of GSEC
NERC	North American Electric Reliability Corporation
NRG	NRG Energy Services, LLC
OPUC	Office of Public Utility Counsel
REP	Retail Electric Provider
SCADA	Supervisory Control and Data Acquisition
SPP	Southwest Power Pool
SPS	Southwestern Public Service Company
TAC	Texas Administrative Code
TOP	Transmission Operator
VOIP	Voice Over Internet Protocol
Xcel	Xcel Energy

Golden Spread Electric Cooperative, Inc. ("GSEC") Emergency Operations Plan Pursuant to 16 TAC § 25.53

1. Approval and Implementation

1.1 Introduction and Applicability

This Emergency Operations Plan ("EOP") is submitted by GSEC in accordance with the rules and requirements outlined in 16 TAC § 25.53(d). GSEC is an electric cooperative with both generation and transmission facilities, therefore it responds to all components of 16 TAC § 25.53(d) with the exception of rules applicable to retail electric providers ("REPs") and Electric Reliability Council of Texas ("ERCOT"), and files annexes to its EOP as applicable in accordance with those required by 16 TAC § 25.53(e)(1) and 16 TAC § 25.53(e)(2).

1.2 GSEC Overview

GSEC is a tax-exempt, consumer-owned Texas Cooperative Corporation, organized in 1984 to supply wholesale electric power to its 16 rural electric distribution cooperative Members ("Members"). Its distribution cooperative Members provide service to about 310,000 electric meters serving their Member-Consumers located in the Panhandle, South Plains and Edwards Plateau regions of Texas, about 24% of the landmass of Texas. Some of these Members also serve areas in the Panhandle of Oklahoma and portions of Kansas and Southeastern Colorado. GSEC serves its 16 Members through its owned-generation resources, market purchases from the Southwest Power Pool ("SPP") and ERCOT, and various agreements it has with transmission service providers and third-party power suppliers.

GSEC owns Mustang Station. It is a six-unit plant located near Denver City, Texas and it has a tested summer output of 921 MW. Mustang Units 1, 2, and 3 make up a 2x1 combined cycle resource, comprised of two natural gas combustion turbines and one steam turbine. Mustang Units 4, 5, and 6 are simple cycle natural gas combustion turbines. In 2011, GSEC added Antelope Station to its generation resources, located near Abernathy, Texas. In 2016, Elk Station was completed and added to the same facility, which is now Antelope Elk Energy Center ("AEEC"). Antelope Station is comprised of three sets of six quick start reciprocating engines, Antelope 1, 2, and 3, with a total tested summer output of 163 MW. Elk Station is comprised of three simple-cycle combustion turbines, Elk 1, 2, and 3, with a total tested summer output of 582 MW. GSEC controls rights to the output of Golden Spread Panhandle Wind Ranch ("GSPWR"), a 78 MW rated wind facility made up of thirty-four wind turbines located near Wildorado, Texas. GSPWR is owned by GSEC's wholly owned affiliate, Golden Spread Panhandle Wind Ranch, LLC. AEEC is GSEC's only generation resource that can operate in the ERCOT market.

GSEC has agreements with NRG Energy Services, LLC ("NRG") and Alliance for Cooperative Energy Services Power Marketing LLC ("ACES") for their generation and market operations services, respectively. NRG operates and maintains each of GSEC's generation facilities, including the maintenance and implementation of each facility's individual EOP. ACES is GSEC's North American Electric Reliability Corporation ("NERC")-registered Generator Operator ("GOP"), power marketer, and single-point-of-contact with GSEC's Reliability Coordinators.

The GSEC Operations Center, operating as an ERCOT Transmission Operator, maintains reliability of its ERCOT Members' Transmission System by using supervisory control and data acquisition ("SCADA") to monitor the transmission system including power flows, voltage, reactive flows, and reactive resources available to maintain the system voltage within limits to protect equipment. The Operations Center is active and available 24/7/365 for continuous communication with ERCOT, its Members, and neighboring utilities.

1.3 EOP Responsibilities

Pursuant to 16 TAC § 25.53(d)(1)(B), the following individuals are responsible for maintaining and implementing components of GSEC's EOP, as well as those who have the authority to change the EOP.

Name	Title	EOP Responsibilities	EOP Section(s)
Stephanie Wells	Compliance Analyst	Maintain, Implement, Authority to Change	1, 1.1, 1.2, 1.3, 1.4, 1.5, 6.1, 7, 8, 9
Andy Stephens	Operations Center Manager	Maintain, Implement, Authority to Change	2.2, 4, 6.1.2, 6.1.2.1, 6.1.2.2, 6.1.2.2.1, 6.1.2.2.2, 6.1.2.2.3, 6.1.2.3, 6.1.2.4, 6.1.2.5, 6.1.2.6, 6.1.2.7, 6.1.2.8, Appendix G
Shane McMinn	Director, Power Delivery	Maintain, Implement, Authority to Change	2.1, 2.2, 4, 6.1.1, 6.1.2, 6.1.2.1, 6.1.2.2, 6.1.2.2.1, 6.1.2.2.2, 6.1.2.2.3, 6.1.2.3, 6.1.2.4, 6.1.2.5, 6.1.2.6, 6.1.2.7, 6.1.2.8, Appendix G
Ty Boatright	Senior Production Asset Manager	Maintain, Implement, Authority to Change	2.3, 6.2.1, 6.2.1.1, 6.2.1.1.1, 6.2.1.1.2, 6.2.1.1.3, 6.2.1.2, 6.2.1.3, 6.2.1.4, 6.2.1.5, 6.2.1.6, 6.2.1.7, Appendix D
Dave Marsh	Senior Production Asset Manager	Maintain, Implement, Authority to Change	2.3, 6.2.2, 6.2.2.1, 6.2.2.1.1, 6.2.2.1.2, 6.2.2.1.3, 6.2.2.2, 6.2.2.3, 6.2.2.4, 6.2.2.5, 6.2.2.6, 6.2.2.7, 6.2.3, 6.2.3.1, 6.2.3.1.1, 6.2.3.1.2, 6.2.3.1.3, 6.2.3.2, 6.2.3.3, 6.2.3.4, 6.2.3.5, 6.2.3.6, 6.2.3.7, Appendix E, Appendix F
Wallace Lester	Safety & Project Coordinator	Maintain, Implement, Authority to Change	3, Appendix A, Appendix C
Lacy Diaz	Human Resources Director	Maintain, Implement, Authority to Change	4, 5

Name	Title	EOP Responsibilities	EOP Section(s)
Alicia Gauna	Information Security Manager	Maintain, Implement, Authority to Change	Appendix B

1.4 Revision Control Summary

Pursuant to 16 TAC § 25.53(d)(1)(C), the following table summarizes the revision control summary for changes made to GSEC's EOP, beginning with the initial filing as required by 16 TAC § 25.53(c)(1). All revisions are reviewed and approved by appropriate executive management prior to implementation.

Revision No.	Date Approved	Summary of Changes
1.0	4/14/2022	Revised all portions of GSEC's EOP to align with the revisions to 16 TAC § 25.53 approved in Project No. 51841.

1.5 Statement on Approval

As of April 14, 2022, Revision No. 1.0 is approved and implemented. This currently approved revision supersedes all previous versions of GSEC's Emergency Operations Plan. This dated statement is provided in accordance with 16 TAC § 25.53(d)(1)(D) and 16 TAC § 25.53(d)(1)(E).

2. Communication Plan

2.1 Overview

Pursuant to 16 TAC § 25.53(d)(2)(A) and 16 TAC § 25.53(d)(2)(B), GSEC is required to have a communications plan for both transmission facilities and generating facilities respectively.

GSEC does not provide retail service to customers or critical load customers. As a result, GSEC does not maintain a process for handling retail customer complaints during an emergency but rather directs those to the appropriate Member who provides the retail service.

The transmission facilities GSEC owns are operated and maintained pursuant to operations and maintenance agreements with the following Members: Big Country Electric Cooperative, Inc.; Coleman Electric Cooperative, Inc.; Concho Valley Electric Cooperative, Inc.; Greenbelt Electric Cooperative, Inc.; South Plains Electric Cooperative, Inc.; and Taylor Electric Cooperative, Inc. GSEC's EOP does not include information regarding the above-mentioned transmission facilities as those facilities fall under the EOPs of the respective operators. Please refer to the EOPs submitted by those cooperatives for the communication procedures required by 16 TAC §25.53(d)(2)(A).

2.2 GSEC Operations Center Communications Plan

16 TAC § 25.53(d)(2)(A) requires an entity with transmission or distribution service operations to describe procedures during an emergency for handling complaints and for communicating with the public; the media; customers; the commission; the Office of Public Utility Counsel ("OPUC"); local and state governmental entities, officials, and emergency operations centers, as appropriate in the circumstances for the entity; the reliability coordinator for its power region; and critical load customers directly served by the entity.

The GSEC Operations Center communicates with its Members, neighboring utilities, ERCOT (reliability coordinator), and the PUCT for a "Significant Interruption" as outlined in Appendix G, SOP-008, Section 5.4.

GSEC does not serve retail customers, therefore the GSEC Operations Center does not communicate directly with retail customers or critical load customers. Any inquiries from the public or government agencies are handled on a case-by-case basis and kept to a minimum.

2.3 Generating Facilities Communications Plan

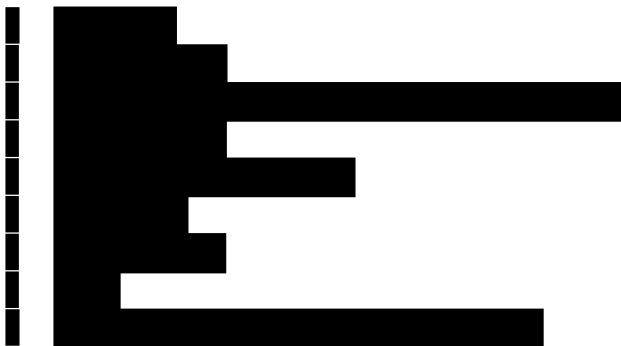
16 TAC § 25.53(d)(2)(B) requires an entity with generation operations to describe the procedures during an emergency for communicating with the media; the commission, OPUC; fuel suppliers, local and state governmental entities, officials, and emergency operations centers, as appropriate in the circumstances for the entity; and the applicable reliability coordinator.



GSEC relies on ERCOT and Southwestern Public Service Company (“SPS”)/Xcel Energy (“Xcel”) for emergency public announcements. Any communication with the media, the commission, local and state government entities, and officials is handled on a case-by-case basis by GSEC and kept to a minimum.

3. Pre-Identified Supplies Plan

Pursuant to 16 TAC § 25.53(d)(3), this section details GSEC’s plan for pre-identified emergency supplies.





4. Emergency Staffing Plan

Pursuant to 16 TAC § 25.53(d)(4), this section outlines GSEC's plan for staffing during emergencies.

GSEC's operations and maintenance contractor, NRG, follows its policies and procedures to operate during potentially severe weather, while at the same time protecting the safety and the integrity of GSEC's generation resources. These procedures shall provide staffing levels during potentially severe weather that will minimize the exposure of GSEC and NRG staff to potentially unsafe conditions, while maintaining reliability of the Bulk Electric Systems. These plans shall also include guidelines to determine when to evacuate the site or shelter in place.



5. Severe-Weather Identification Plan

Pursuant to 16 TAC § 25.53(d)(5), this section outlines GSEC's plan for identification of severe weather threats.



6. Annexes Pursuant to 16 TAC § 25.53(e)

6.1 Transmission Facility Annexes

Pursuant to 16 TAC § 25.53(e)(1), GSEC is required to include in its EOP the outlined annexes for its transmission and distribution facilities. GSEC does not own or operate any distribution facilities, but GSEC has two types of transmission facilities: transmission facilities GSEC owns but are operated and maintained pursuant to operations and maintenance agreements with certain Members, as described in Section 6.1.1, and the GSEC Operations Center, as described in Section 6.1.2.

6.1.1 Transmission Facilities

The transmission facilities GSEC owns are operated and maintained pursuant to operations

and maintenance agreements with the following Members: Big Country Electric Cooperative, Inc.; Coleman Electric Cooperative, Inc.; Concho Valley Electric Cooperative, Inc.; Greenbelt Electric Cooperative, Inc.; South Plains Electric Cooperative, Inc.; and Taylor Electric Cooperative, Inc. GSEC's EOP does not cover the above-mentioned transmission facilities. Please refer to these Members' filed EOPs for annexes required by 16 TAC § 25.53(e)(1) related to these facilities.

6.1.2 GSEC Operations Center

Pursuant to 16 TAC § 25.53(e)(1), the following sub-sections include annexes for the GSEC Operations Center.

6.1.2.1 Weather Emergency Annex

While 16 TAC § 25.53(e)(1)(A) requires entities with transmission facilities to file a weather emergency annex that includes operational plans for responding to a cold or hot weather emergency as well as checklists for transmission facility personnel, this requirement is not applicable to the GSEC Operations Center. The GSEC Operations Center is located within the GSEC Headquarters, and operates 24/7/365, regardless of weather. GSEC does not field-operate or maintain any transmission facilities such as transmission lines or substations, thus there are no GSEC transmission facilities to prepare for an imminent cold or hot weather emergency.

6.1.2.2 Load Shed Annex

Pursuant to 16 TAC § 25.53(e)(1)(B), the following sub-sections outline GSEC's Load Shed Annex for the GSEC Operations Center.

6.1.2.2.1 Curtailment Priorities, Load Shed Procedures, Rotating Outages and Planned Interruptions

Pursuant to 16 TAC § 25.53(e)(1)(B)(i), the following section outlines GSEC's procedures for controlled shedding of load.

SPP:

The SPP Emergency Operations Plan, Section 6.3.3.1, requires that Load Serving Entities ("LSE") have manual load shedding plans. Accordingly, GSEC has developed an Emergency Load Curtailment Program ("ELCP") for allocation of required load curtailment to its Members.

The SPP Balancing Authority ("BA") or applicable Transmission Operator ("TOP") may determine that system reliability requires a manual load curtailment and will allocate GSEC's requirement. In the event GSEC receives a directive from the SPP BA or an applicable TO to shed load, the SPS TOP will allocate GSEC's load shed responsibility on a load ratio share basis to all entities involved. GSEC has given the SPS TOP the authority to curtail all SPP Members with allocation of load curtailment determined by their current real time load ratio share. Each Member cooperative will be notified by the SPS TOP of their required load curtailment. Each individual Member determines the need for curtailment priorities, rotating outages, and planned interruptions.

GSEC provides real time SCADA load data of each of its Members for use by the SPS TOP to calculate the load ratio share of GSEC as a whole in a load shed event, and to

calculate each individual Member's responsibility.

The SPS TOP will contact each GSEC Member of their load shed requirement.

ERCOT:

Appendix G contains GSEC SOP-013 Manual Load Shedding Procedure and GSEC SOP-15 Underfrequency Load Shed Procedure, both of which address load shed procedures. The ERCOT Nodal Operating Guide, Section 4.5.3.4, obligates Distribution Service Providers to shed load when notified by ERCOT through their ERCOT TO. GSEC is its Members (in ERCOT) designated TO. Each individual Member determines the need for curtailment priorities, rotating outages, and planned interruptions.

6.1.2.2.2 Priorities for Restoration of Service

Pursuant to 16 TAC § 25.53(e)(1)(B)(ii), the following section outlines GSEC's priorities for restoring shed load to service.

SPP:

The amount of restoration to each Member is determined by the SPP Reliability Coordinator and communicated to the TOP (SPS). The SPS TOP will notify each Member what percentage of previously shed load can be restored. Priority of restoration for each Member-consumer is determined by each Member.

ERCOT:

Appendix G contains GSEC SOP-013 Manual Load Shedding Procedure and GSEC SOP-15 Underfrequency Load Shed Procedure, both of which address load shed procedures. GSEC's Transmission Operations Center will notify each Member what percentage of previously shed load can be restored. Priority of restoration for each Member-consumer is determined by each Member.

6.1.2.2.3 Registry of Critical Load Customers

16 TAC § 25.53(e)(1)(B)(iii) requires a procedure for maintaining an accurate registry of critical load customers directly served if maintained by the entity. GSEC does not serve retail electric service customers and therefore provides no direct service to critical load customers. GSEC provides wholesale service to its Members, who sell at retail to their Member-consumers.

6.1.2.3 Pandemic and Epidemic Annex

In accordance with 16 TAC § 25.53(e)(1)(C), Appendix A contains the GSEC Pandemic Preparedness Plan. This plan begins with preparatory actions to protect GSEC staff from infection, continues through the event and subsequent recovery.

6.1.2.4 Wildfire Annex

While 16 TAC § 25.53(e)(1)(D) requires a wildfire annex for transmission facilities, the GSEC Operations Center is located in the GSEC Headquarters facility. GSEC office facilities are located in urban areas where the risk of damage from wildfires is minimal.

6.1.2.5 Hurricane Annex

GSEC and its Members do not own, maintain, or control facilities located within a hurricane evacuation zone as defined by the TDEM, thus 16 TAC § 25.53(e)(1)(E) is not

applicable.

6.1.2.6 Cyber Security Annex

In accordance with 16 TAC § 25.53(e)(1)(F), Appendix B contains the GSEC Cyber Security Annex, composed of GSEC's Incident Reporting and Response Plan.

6.1.2.7 Physical Security Incident Annex

In accordance with 16 TAC § 25.53(e)(1)(G), Appendix C contains the GSEC Physical Security Incident Annex, composed of GSEC's Emergency Action Plan.

6.1.2.8 Use of Facilities Under PURA § 39.918(b)(1) & (2)

GSEC is an electric cooperative, not a transmission and distribution utility, thus 16 TAC § 25.53(e)(1)(H) is not applicable.

6.2 Generating Facility Annexes

6.2.1 Mustang Station

The emergency procedures for Mustang Station are included in Appendix D.

6.2.1.1 Weather Emergency Annex

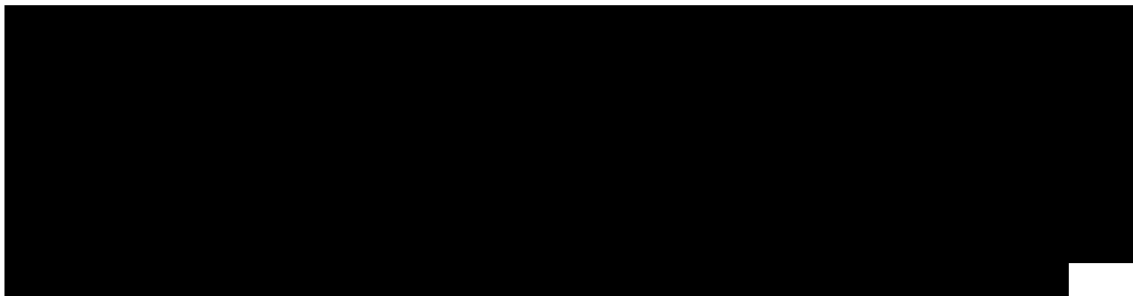
Pursuant to 16 TAC § 25.53(e)(2)(A), the following sub-sections outline GSEC's weather emergency annex for Mustang Station.

In addition to the 16 TAC § 25.53(e)(2)(A) required procedures for cold or hot weather emergencies outlined in Section 6.2.1.1.1, Mustang Station has a Tornado/High Wind Event emergency operating procedure included in Appendix D, EOP-11, and a Wildfire Procedure, EOP-12.

6.2.1.1.1 Cold or Hot Weather Emergency

Pursuant to 16 TAC § 25.53(e)(2)(A)(i), this section outlines GSEC's operational plans for responding to a cold or hot weather emergency at Mustang Station. Appendix D contains Mustang Station EOP-9 procedure for addressing severely cold weather, and Mustang Station EOP-10 procedure for addressing severely hot weather. These procedures contain plans distinct from the weather preparations required under 16 TAC §25.55.

6.2.1.1.2 Fuel Switching Equipment



6.2.1.1.3 Emergency Checklists

Pursuant to 16 TAC § 25.53(e)(2)(A)(iii), GSEC has checklists for generation resource personnel at Mustang Station to use during a cold or hot weather emergency response. These checklists can be found in Appendix D, in EOP-9 and EOP-10, the procedures for

severely cold and severely hot weather, respectively.

In addition to checklists for cold or hot weather emergencies, Mustang Station has checklists included in Appendix D EOP-11 and EOP-12, the procedures for tornado/high wind events and wildfires, respectively.

6.2.1.2 Water Shortage Annex

Pursuant to 16 TAC § 25.53(e)(2)(B), Appendix D contains the Mustang Station EOP-13 procedure that addresses a site water shortage.

6.2.1.3 Pandemic and Epidemic Annex

In accordance with 16 TAC § 25.53(e)(2)(D), Appendix A contains the GSEC Pandemic Preparedness Plan. This plan begins with preparatory actions to protect GSEC staff from infection, continues through the event and subsequent recovery. This plan is used at Mustang Station in addition to any NRG-specific pandemic response processes in place at the facility.

6.2.1.4 Hurricane Annex

GSEC and its Members do not own, maintain, or control facilities located within a hurricane evacuation zone as defined by TDEM, thus 16 TAC § 25.53(e)(2)(E) is not applicable.

6.2.1.5 Cyber Security Annex

In accordance with 16 TAC § 25.53(e)(2)(F), Appendix B contains the GSEC Cyber Security Annex, composed of GSEC's Incident Reporting and Response Plan. This plan is used at Mustang Station in addition to any NRG-specific cyber security response processes in place at the facility.

6.2.1.6 Restoration of Service Annex

Pursuant to 16 TAC § 25.53(e)(2)(C), Appendix D contains the Mustang Station EOP-14 procedure that addresses how personnel plan to restore to service Mustang Station after it fails to start or tripped offline due to a hazard or threat. Additionally, Mustang Station has specific procedures for a gas turbine trip, EOP-2, and steam turbine generator trip, EOP-4, in Appendix D.

6.2.1.7 Physical Security Incident Annex

In accordance with 16 TAC § 25.53(e)(2)(G), Appendix C contains the GSEC Physical Security Incident Annex, composed of GSEC's Emergency Action Plan. This plan is used at Mustang Station in addition to any NRG-specific physical security processes in place at the facility.

6.2.2 AEEC

The emergency procedures for AEEC are Section 12 of the AEEC Operating Manual and included in Appendix E.

6.2.2.1 Weather Emergency Annex

Pursuant to 16 TAC § 25.53(e)(2)(A), the following sub-sections outline GSEC's weather emergency annex for AEEC.

In addition to the 16 TAC § 25.53(e)(2)(A) required procedures for cold or hot weather

emergencies outlined in Section 6.2.2.1.1, AEEC has a Severe Weather and Natural Disasters emergency operating procedure included in Appendix E, Section 12.7, and an Area Wildfire Procedure, Section 12.19.

6.2.2.1.1 Cold or Hot Weather Emergency

Pursuant to 16 TAC § 25.53(e)(2)(A)(i), this section outlines GSEC's operational plans for responding to a cold or hot weather emergency at AEEC. Appendix E contains Sections 12.16 and 12.17 which are AEEC's procedures for addressing severely cold and hot weather, respectively. These procedures contain plans distinct from the weather preparations required under 16 TAC § 25.55.

6.2.2.1.2 Fuel Switching Equipment



6.2.2.1.3 Emergency Checklists

Pursuant to 16 TAC § 25.53(e)(2)(A)(iii), GSEC has checklists for generation resource personnel at AEEC to use during a cold or hot weather emergency response. These checklists can be found in Appendix E, in Section 12.16 and 12.17, the AEEC procedures for severely cold and severely hot weather, respectively.

In addition to checklists for cold or hot weather emergencies, AEEC has checklists for other emergency procedures included in Appendix E.

6.2.2.2 Water Shortage Annex

Pursuant to 16 TAC § 25.53(e)(2)(B), Appendix E contains Section 12.18, the AEEC procedure that addresses a site water shortage.

6.2.2.3 Restoration of Service Annex

Pursuant to 16 TAC § 25.53(e)(2)(C), Appendix E contains Section 12.14, the AEEC procedure that addresses how personnel plan to restore to service AEEC after it fails to start or tripped offline due to a hazard or threat.

6.2.2.4 Pandemic and Epidemic Annex

In accordance with 16 TAC § 25.53(e)(2)(D), Appendix A contains the GSEC Pandemic Preparedness Plan. This plan begins with preparatory actions to protect GSEC staff from infection, continues through the event and subsequent recovery. This plan is used at AEEC in addition to the AEEC-specific Pandemic Plan in Section 12.24 of Appendix E.

6.2.2.5 Hurricane Annex

GSEC and its Members do not own, maintain, or control facilities located within a hurricane evacuation zone as defined by TDEM, thus 16 TAC § 25.53(e)(2)(E) is not applicable.

6.2.2.6 Cyber Security Annex

In accordance with 16 TAC § 25.53(e)(2)(F), Appendix B contains the GSEC Cyber Security Annex, composed of GSEC's Incident Reporting and Response Plan. This plan is used at AEEC in addition to the AEEC-specific Cyber Disruption procedure in Section 12.8 of Appendix E.

6.2.2.7 Physical Security Incident Annex

In accordance with 16 TAC § 25.53(e)(2)(G), Appendix C contains the GSEC Physical Security Incident Annex, composed of GSEC's Emergency Action Plan. This plan is used at AEEC in addition to any NRG-specific physical security processes in place at the facility.

6.2.3 GSPWR

The emergency procedures for GSPWR are included in Appendix F.

6.2.3.1 Weather Emergency Annex

Pursuant to 16 TAC § 25.53(e)(2)(A), the following sub-sections outline GSEC's weather emergency annex for GSPWR.

In addition to the 16 TAC § 25.53(e)(2)(A) required procedures for cold or hot weather emergencies outlined in Section 6.2.3.1.1, GSPWR has emergency action plans for other weather emergencies in Section 16.0 of the GSPWR Emergency Action Plan in Appendix F.

6.2.3.1.1 Cold and Hot Weather Emergency

Pursuant to 16 TAC § 25.53(e)(2)(A)(i), this section outlines GSEC's operational plans for responding to a cold or hot weather emergency at GSPWR. Appendix F contains the GSPWR Site Weather Procedure for addressing cold and hot weather emergencies, which is distinct from the weather preparations required under 16 TAC § 25.55.

6.2.3.1.2 Fuel Switching Equipment



6.2.3.1.3 Emergency Checklists

16 TAC §-25.53(e)(2)(A)(iii) requires checklists for generation resource personnel to use during a cold or hot weather emergency. The GSPWR Site Weather Procedure and Emergency Action Plan in Appendix F provide general and checklist instructions for summer and winter operations and other weather-related emergencies.

6.2.3.2 Water Shortage Annex

16 TAC §-25.53(e)(2)(B) requires a procedure for addressing supply shortages of water used in the generation of electricity. This requirement is not applicable to GSPWR as the operational water requirements at GSPWR are minimal.

6.2.3.3 Restoration of Service Annex

Pursuant to 16 TAC §-25.53(e)(2)(C), Appendix F contains GSPWR-OPS-07, the GSPWR Restoration of Service plan that addresses how personnel plan to restore to service GSPWR after it fails to start or tripped offline due to a hazard or threat.

6.2.3.4 Pandemic and Epidemic Annex

In accordance with 16 TAC § 25.53(e)(2)(D), Appendix A contains the GSEC Pandemic Preparedness Plan. This plan begins with preparatory actions to protect GSEC staff from infection, continues through the event and subsequent recovery. This plan is used at GSPWR in addition to any NRG-specific pandemic response processes in place at the facility.

6.2.3.5 Hurricane Annex

GSEC and its Members do not own, maintain, or control facilities located within a hurricane evacuation zone as defined by TDEM, thus 16 TAC § 25.53(e)(2)(E) is not applicable.

6.2.3.6 Cyber Security Annex

In accordance with 16 TAC § 25.53(e)(2)(F), Appendix B contains the GSEC Cyber Security Annex, consisting of GSEC's Incident Reporting and Response Plan. This plan is used at GSPWR in addition to any NRG-specific cyber security processes in place at the facility.

6.2.3.7 Physical Security Incident Annex

In accordance with 16 TAC § 25.53(e)(2)(G), Appendix C contains the GSEC Physical Security Incident Annex, consisting of GSEC's Emergency Action Plan. This plan is used at GSPWR in addition to any NRG-specific physical security processes in place at the facility.

7. Drills

In accordance with 16 TAC § 25.53(f), GSEC is required to test its EOP at least once per a calendar year unless its EOP has been activated. However, due to the guidance provided by PUCT Commission Staff during the March 11, 2022 workshop GSEC is not performing a drill prior to the initial filing required by 16 TAC § 25.53(c)(1). GSEC tentatively plans to perform a test of its EOP by Fall 2022.

8. Reporting Requirements

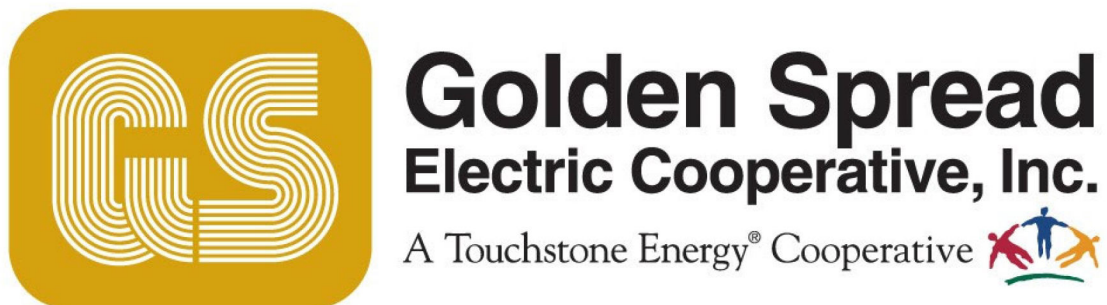
GSEC will comply with all reporting requirements pursuant to 16 TAC § 25.53(g). In the event the Texas State Operations Center (SOC) is activated, GSEC will provide updates on the status of operations, outages, and restoration efforts as requested to PUCT staff. The emergency contacts on file with the PUCT and included in GSEC's Executive Summary will respond to any inquiries from the PUCT.

9. Copy Available for Inspection

In accordance with 16 TAC § 25.53(c)(1)(D), GSEC will make its unredacted EOP available in its entirety to PUCT Commission Staff on request at a location designated by PUCT Commission Staff.

Appendix A

Pandemic Preparedness Plan



PANDEMIC PREPAREDNESS PLAN

[illegible]

Age Group	Percentage
18-24	10%
25-34	20%
35-44	30%
45-54	35%
55-64	25%
65-74	15%
75-84	10%
85+	5%

[REDACTED]

[REDACTED]

██████████

5.1 EPIDEMIC STATUS REQUIREMENTS

[REDACTED]

6.1 PANDEMIC STATUS REQUIREMENTS

[REDACTED]

[Redacted]

7.1 GSEC Coordination/Monitoring

[Redacted]

[Redacted]

[Redacted]

7.2 Post-Pandemic Evaluation

[Redacted]

[Redacted]		
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]		
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]		
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



7.2 Annual Preparation



7.5 Additional Resources

The following websites provide additional infectious disease planning and response information:

Centers for Disease Control and Prevention

<http://www.cdc.gov/flu/>

PandemicFlu.gov

<http://www.pandemicflu.gov>

<http://www.pandemicflu.gov/plan/> (Planning Templates)

U.S. Department of Health & Human Services

<http://www.hhs.gov/pandemicflu/plan/> (US Response Plan)

<http://www.hhs.gov/flu/> (Information on Seasonal Flu)

World Health Organization

<http://www.who.int/topics/influenza/en/index.html>

North American Electric Reliability Council (NERC)

<http://www.nerc.com/docs/cip/Influenza%20Pandemic%20Reference%20Guide.pdf>

Appendix B

Cyber Security Plan



**Golden Spread
Electric Cooperative, Inc.**

A Touchstone Energy® Cooperative 

Incident Reporting And Response Plan

INCIDENT REPORTING AND RESPONSE PLAN

1 PURPOSE

The purpose of this Incident Reporting and Response Plan (“IRRP”) is to provide a process for Golden Spread Electric Cooperative, Inc.’s (“GSEC”) that is formal, focused, and coordinated approach to responding to security events categorized as either cyber or physical security incidents.

This IRRP ensures that incidents are responded to in a systematic approach that is consistent with GSEC’s overall objectives and strategies. The plan ensures communication efforts to appropriate federal agencies, law enforcement agencies, shareholders, customers, and the media are defined, focused, and controlled. The plan will also ensure consistent incident handling and response and provides for future development and refinement of security controls.

2 SCOPE

The IRRP is applicable to all personnel who have been identified to have direct or indirect assigned duties for GSEC. GSEC maintains physical and cyber security best practices. These best practices are based on the NIST Cybersecurity Framework.

3 GOALS

GSEC works to promote resilience and enhance cyber security capabilities and works to convey current information on emerging cyber threats and initiatives, including critical infrastructure protection efforts, and realistic practices for improving operational resilience. The information technology team will keep Members and staff informed while maintaining a working partnership amongst the various cooperative functional groups on matters of cyber security.

Short Term Goals:

- Identify gaps in cyber management practices and recommend process improvements.
- Reinforce cyber security best practices and examine resilience concepts and objectives.
- Discuss processes to maintain and repeatedly carry out protection and sustainment activities for critical assets and services.
- Share information with cooperative functional groups related to cyber security policies, initiatives, and capabilities.

Long Term Goals:

- Address gaps in cyber management practices and implement process improvements.
- Document a process to maintain and repeatedly carry out protection and sustainment activities for critical assets and services.
- Enhance cyber incident response and business continuity capabilities.
- Increase the cybersecurity maturity and resilience of the cooperative.

4 ROLES AND RESPONSIBILITIES

This Incident Reporting and Response Plan must be followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of GSEC. All personnel are referred to as staff within this plan.

Below are details about the roles and responsibilities of each Member to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Appendix A lists the departments and teams who currently assist with incident response.

4.1 Incident Response Lead

The Incident Response lead is responsible for:

- Making sure that the Security IRRP and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
- Making sure that the Security IRRP is current, reviewed and tested at least once each year.
- Making sure that staff with Security IRRP responsibilities are properly trained at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security IRRP when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

4.2 Security Incident Response Team (SIRT)

The Security Incident Response Team (SIRT) is responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

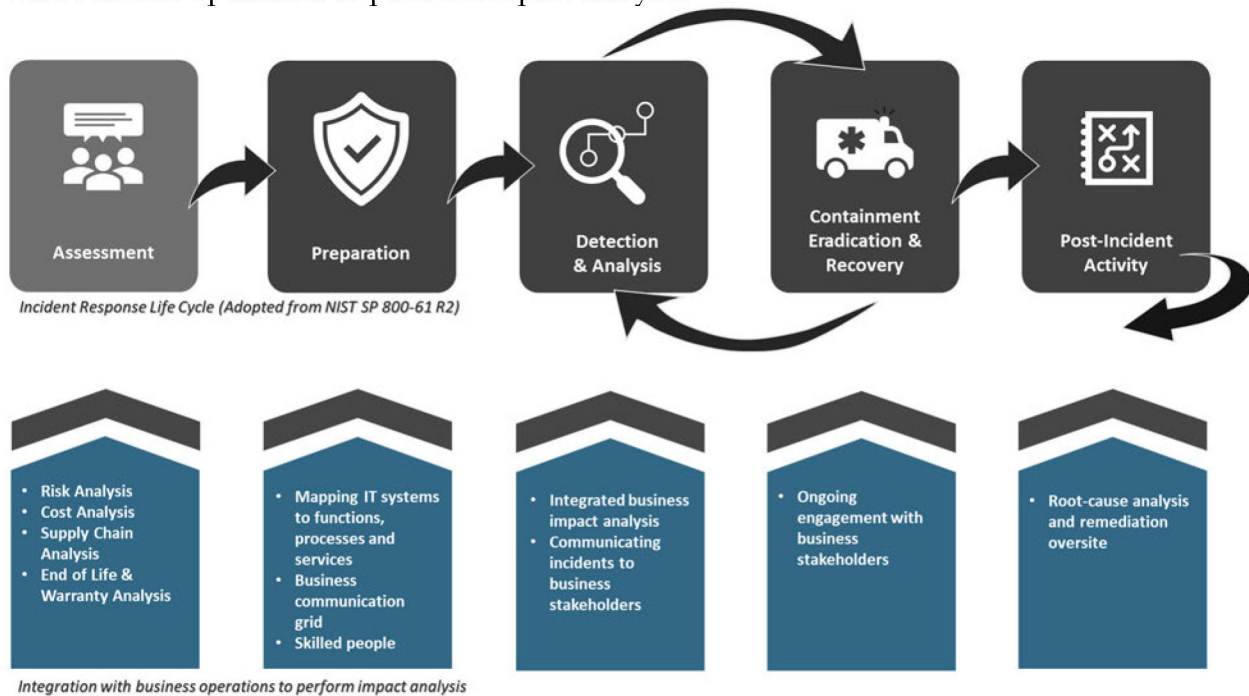
4.3 All Staff Members

All Staff Members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the SIRT.
- Reporting any security related issues or concerns to management, or to a member of the SIRT.
- Complying with the security policies and procedures of GSEC.

5 INCIDENT RESPONSE LIFE CYCLE

This Incident Response Plan is designed to provide a Cooperative-wide, systematic business approach to the Incident Response Life Cycle. The Incident Response Life Cycle is paralleled with business operations to perform impact analysis.



5.1 Life Cycle Objectives and Processes

5.1.1 Assessment

Establish an approach to analyze business impact and risk. Perform a risk analysis Cooperative wide and understand what assets and resources must be protected. Determine operational and financial risks that could impact business operations in the event of a security incident. Regularly review supply chain risk and vulnerability management assessments.

5.1.2 Preparation

Establish an approach to incident handling that includes development of policy and procedures. Review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a SIRT.

5.1.3 Detection and Analysis

Analyze detection devices and reports from people to identify and classify the activity and begin handling the evidence. Monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

5.1.4 Containment

Ensure the impact of the incident does not increase. Perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

5.1.5 Eradication

Determine the cause and remove it. Remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

5.1.6 Recovery

Restore the system to its original state and validate the clean system. bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

5.1.7 Post-Incident Activity

Develop follow-up reports, identify lessons learned, and update procedures as necessary. No later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved. In some instances, documentation may be needed for compliance requirements.

5.2 Integration of Business Operations

Develop a risk register which includes the systems and processes necessary to continue business operations and the impacts of each in the event systems are not available. The risk register should also include a list of contacts. The integration of business operations will assist incident handlers and stakeholders with identifying potential risks and associated services along the incident response life cycle. The risk register and contact lists should be kept as a hard copy for reference when systems are not available.

6 INCIDENT SCORING AND IMPACT RATING

GSEC uses a weighted arithmetic mean to produce a score from zero to 10. This score drives the incident triage and escalation processes and assists in determining the prioritization of limited incident response resources and the necessary level of support for each incident.

(Current Functional Impact * 40%) + (Potential Functional Impact * 25%) + (Informational Impact * 10%) + (System Criticality * 20%) + (Recoverability Timeframe * 5%) = The Incident Score

The five factors are assigned values between 0 and 10 based on value assigned the individual severity rating for each of the factors as described in this plan using the formula above.

The purpose of weighting the factors is to provide a repeatable formula that is heavily biased by the actual impact of the incident but also considers potential impacts to GSEC if the incident were not contained guide appropriate actions with sufficient urgency to prevent a minor or moderate incident from escalating into an emergency.

7 Incident Categorization

7.1 CAT 1 UNAUTHORIZED ACCESS

Physical

1. Could the incident impact the reliability of the bulk power system?
2. Was there intentional damage to security systems that protect the physical perimeter.
3. Was sensitive information lost or removed without authorization. Was social engineering involved?

Cyber

1. Could the incident impact GSEC? Was social engineering involved? Was sensitive information copied, transmitted, viewed, stolen or used by an unauthorized individual?
2. Was this an attempt to compromise GSEC either electronically or physically? (*report within 1 hour*)

7.2 CAT 2 DENIAL OF SERVICE

1. Was malicious software or data modification discovered on a cyber asset or assets that may impact the reliability of the bulk power system?
2. Was social engineering involved?
3. If yes to any of these questions report to E-ISAC within the listed timeframe

7.3 CAT 3 MALICIOUS CODE

1. Was malicious software or data modification discovered on a cyber asset or assets that may impact the reliability of GSEC?
2. Was social engineering involved?

7.4 CAT 4 IMPROPER USAGE

1. Was social engineering involved?
2. Did an unauthorized employee access confidential or restricted resources?

7.5 CAT 5 SCANS/PROBES/ATTEMPTED ACCESS/SURVEILLANCE/THREATS

Physical

1. Was this an attempt to compromise GSEC either electronically or physically?
2. Was suspicious photo taking observed?
3. Were suspicious surveillance activities observed?
4. Was a suspicious fly over observed?
5. Was a threat communicated where the threatened action has the potential to damage or compromise facility or personnel?
6. Were explosives discovered at or near a facility?
7. Were there suspected or actual attacks against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel?

7.6 CAT 6 INVESTIGATION

1. Could the incident impact the reliability of GSEC?
2. Is there targeted, focused, or repetitive attempted access to cyber assets (such as critical cyber assets) whose impairment could impact bulk power system reliability?
3. Was social engineering involved?
4. Was a threat communicated where the threatened action has the potential to damage or compromise facility or personnel?
5. Was this an attempt to compromise the bulk power system either electronically or physically?

8 INCIDENT REPORTING GUIDELINES

8.1 Reporting Forms (Internal)

Incident reports are collected in GSEC's IT ticketing system with supporting documentation and communications. In most cases, reporting will also include lessons learned and after actions reports.

8.2 Reporting Agency Forms (External)

8.2.1 Department of Energy (DoE) Required Respondents (taken from the DoE website)

Electric utilities that operate as Control Area Operators and/or Reliability Authorities as well as other electric utilities, as appropriate, are required to file the form. The form is a mandatory filing whenever an electrical incident or disturbance is sufficiently large enough to cross the reporting thresholds. Reporting coverage for the Form DOE-417 includes all 50 States, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and the U.S. Trust Territories.

Electric Disturbance Events (DOE-417)

Online Form: <https://www.oe.netl.doe.gov/OE417/>

Downloadable PDF Form:

https://www.oe.netl.doe.gov/docs/OE417_Form_05312024.pdf

Offline Reporting: If you are unable to submit online or by fax, forms may be e-mailed to doehqeoc@hq.doe.gov, or call and report the information to the following telephone number: (202) 586-8100.

8.2.2 Electricity Information Sharing and Analysis Center (E-ISAC)

The Electricity Information Sharing and Analysis Center (E-ISAC) provides GSEC an option to add a physical or cyber bulletin posting for information sharing purposes. An account must be created and approved for sharing information. Information shared may include details about a security incident attack and the Indicators of Compromise (IoC) to assist other cooperatives with mitigation of similar attacks.

E-ISAC website login: <https://www.eisac.com>

8.2.3 Electric Reliability Council of Texas (ERCOT)

Market participants must notify ERCOT as soon as practical upon determination of a cybersecurity incident on a Market Participant's computer network or system that interfaces with an ERCOT computer network or system, the Market Participant shall notify ERCOT.

8.3 What to Include in your Incident Report

The following format is a guide. While internal reporting must be complete, some external reports may need to omit certain pieces of information to retain confidentiality. External reporting should be reviewed by managers, senior leadership, and sometimes legal counsel.

The following must be determined for each incident:

- Incident Type
- Names of system(s) involved (spell out each acronym used at its first use)
- If the system has failed over to an available backup system
- Categorization of system(s) involved
- Type of data involved (Confidential or Restricted Information)
- Functional use of systems involved
- Identified or suspected cause of incident

- Identified or suspected impact of incident
- What dangers or effects on the facility or facility personnel safety may be caused by the event?
- If the incident has the potential to spread across other networks or even outside to partners or customers
- Investigation, containment, and remediation steps taken
- Incident detection/identification method
- Parties involved (include descriptive titles and names if required for remediation)
- Date and timeframe of occurrence(s)
- If the reported incident is real or a false positive
- What stage the incident is in – beginning, in process, or has already occurred
- What organizations will be affected and who should be part of the response.

If applicable, provide:

- Host-based indicators, Network indicators, and Email characteristics
- Security controls that blocked and/or detected the activity
- Date/time the activity was blocked and/or detected
- Host operating systems
- Name of malicious logic
- How did the exploit occur, and can it happen again? In what timeframe?
- What type of attacker tools if any were placed onto the system?
- Actions taken by affected system
- Network activity observed (including IPs and URLs connections made or attempted, associated ports)
- Type of unauthorized access attempted or obtained (including capabilities associated with that type of access)
- Attack vector

For incidents involving privacy or PII, also include:

- The number of individuals
- The number of records
- The number of data points or source of compromise

9 COMMUNICATIONS

9.1 Internal Reporting Chain

GSEC's Internal Reporting Chain during an incident is based on the severity rating. If a member of the reporting chain is unavailable, their designated delegate will be contacted. If both the primary and their delegate cannot be contacted, the next person in the chain will be notified. All members of the chain must select a delegate.

Severity	Reporting Guidance
Insignificant	Reporting is not necessary

Severity	Reporting Guidance
Low	The Incident Response Lead will notify the Information Security Manager who then decides whether or not to notify the Director of IT Security who then decides whether or not to notify the General Manager.
Medium	The Incident Response Lead will notify the Information Security Manager who then notifies the Director of IT Security who then decides whether or not to notify the General Manager.
High	<p>The Incident Response Lead will notify the Information Security Manager who then notifies the Director of IT Security who then notifies the General Manager. The ISM also informs other departments that have a need to know.</p> <p>At this severity level, the ISM will establish a Virtual channel for incident handling activities understanding that Confidential or Restricted Information is not stored or shared via the channel.</p>
Extreme	<p>The Incident Response Lead will notify the Information Security Manager who then notifies the Director of IT Security who then notifies the President and Chief Executive Officer. The ISM also informs other departments that have a need to know.</p> <p>At this severity level, the ISM will establish a Virtual channel for incident handling activities understanding that Confidential or Restricted Information is not stored or shared via the channel.</p>

9.2 External Reporting Chain

Name	Email	Phone
Electric Reliability Council of Texas (ERCOT)	<p><u>Reporting Form:</u> <u>https://www.ercot.com/files/docs/2022/04/01/16-040122_Nodal.docx</u></p> <p>If form cannot be accessed, email information to <u>NCSI@ercot.com</u></p>	(512) 248-6800
Department of Energy (DOE)	<p><u>https://www.oe.netl.doe.gov/OE417/</u></p> <p>FAX Form DOE-417 to (202) 586-8485 Email Form DOE-417 to <u>doehgeoc@hq.doe.gov</u></p>	(202) 586-8100
E-ISAC	<u>operations@eisac.com</u>	404-446-9780 #2
Federal Bureau of Investigation (FBI)	<u>dallas.fbi.gov</u>	972-559-5000
NCCIC (includes ICS-CERT and US-CERT)	<p><u>central@cisa.gov</u></p> <p>Online form: <u>https://us-cert.cisa.gov/forms/report</u></p>	1-888-282-0870
ICS-CERT	<p><u>soc@us-cert.gov</u></p> <p>online form: <u>https://us-cert.cisa.gov/forms/report</u></p>	1-888-282-0870

US-CERT	soc@us-cert.gov online form: https://us-cert.cisa.gov/forms/report	1-888-282-0870
Department of Homeland Security, Cyber Security Regional Contact	Chad Adams CISARegion6@hq.dhs.gov	1-888-282-0870

9.3 Key Vendor Contacts

Key Vendor contacts are kept by the SIRT team in a centralized location.

9.4 Media Communications

Only employees authorized by the President and CEO and his or her designee are permitted to speak to, give statements to, or participate in interviews with members of the news media as an official representative of GSEC.

By default, employees are not authorized by the President and CEO to communicate with the news media as an official representative of GSEC and should refer any news media enquiries to an authorized employee.

9.5 Impaired Communications

GSEC will identify another means to establish communications in the event that communications are disrupted. GSEC will utilize cell phones, networks, the internet, etc.

10 FORENSICS

GSEC, when deemed necessary to investigate possible criminal activity, will provide forensic services and it is not intended for law enforcement or to be court admissible. If it is determined that forensics be conducted, the cooperative shall require a dedicated evidence storage and analysis facilities with physical access limited to authorized forensics personnel, mobile evidence gathering tools required to establish chain of custody; to collect and label evidence at incident sites; and to securely package and transport the collected evidence. GSEC shall: Develop, maintain, and follow a Standard Operating Procedure (SOP) for computer forensics collection and analysis follow GSEC disclosure and privacy guidance and maintain a chain of custody of evidence. In the event that law enforcement services are required, the Incident Response Lead makes initial contact with senior leadership, legal and law enforcement organizations to establish evidentiary chain of custody. The Incident Response Lead will coordinate with appropriate law enforcement organizations. If necessary, GSEC or the Incident Response Lead may package and ship equipment to a designated computer forensic processing facility. If it is determined that the source of the suspected criminal activity is external to GSEC, the appropriate law enforcement organization will be notified immediately by the Incident Response Lead, or if necessary, by other organizations who will inform GSEC at the earliest time possible.

11 TESTING AND PLAN CHANGES

The Incident Reporting and Response Plan will be reviewed and tested at least once every 24 calendar months for updates and improvements. GSEC reserves the right to modify or amend this policy at any time, with or without prior notice. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, lessons learned, or the absence of any lessons learned will be documented. The Incident Reporting and Response Plan will be updated and distributed to those individuals with a documented role and responsibility in the IRRP via email based on any documented lessons learned associated with the plan. If roles and responsibilities change or if there is a technology change that impacts GSEC's ability to execute the plan, the Incident Reporting and Response Plan will be updated and each person with a defined role and responsibility in the IRP will be notified

via email.

12 TRAINING REQUIREMENTS FOR INCIDENT RESPONSE TEAMS

Training requirements for the incident handlers includes:

- Intrusion Detection System training
- Security Information and Event Management training (if applicable)
- Ticketing/ Reporting system
- Additional security monitoring and reporting tools as necessary
- Regular review of the Incident Response and Reporting Plan
- Cybersecurity Framework for all areas of GSEC
- Communications applications (Teams, etc.)
- Practice with locating and filling out External Agency reports (DoE, E-ISAC, etc.)

13 ROADMAP FOR MATURING THE INCIDENT RESPONSE CAPABILITY

GSEC will follow the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), to define their roadmap for maturity in Incident Reporting and Response Planning.

Appendix A – ASSIGNED ROLES

Role	Departments/Team(s)
Incident Response Lead	Information Security Manager
Security Incident Response Team (SIRT)	SOC Personnel, Network Team, Systems Team, End-User Support Team, Cyber Insurance Contact

Appendix B – Incident Response Plan Checklist

Response

Responding to security incidents can take several forms. Incident response actions may include triaging alerts from your endpoint security tools to determine which threats are real and/or the priority in which to address security incidents. Incident response activities can also include containing and neutralizing the threat(s)—isolating, shutting down, or otherwise “disconnecting” infected systems from your network to prevent the spread of the cyber attack. Additionally, incident response operations include eliminating the threat (malicious files, hidden backdoors, and artifacts) which led to the security incident.

- Immediately contain systems, networks, data stores and devices to minimize the breadth of the incident and isolate it from causing wide-spread damage.
- Determine if any sensitive data has been stolen or corrupted and, if so, what the potential risk might be to your business.
- Eradicate infected files and, if necessary, replace hardware.
- Keep a comprehensive log of the incident and response, including the time, data, location and extent of damage from the attack. Was it internal, external, a system alert, or one of the methods described previously? Who discovered it, and how was the incident reported? List all the sources and times that the incident has passed through. At which stage did the security team get involved?
- Preserve all the artifacts and details of the breach for further analysis of origin, impact, and intentions.
- Prepare and release public statements as soon as possible, describe as accurately as possible the nature of the breach, root causes, the extent of the attack, steps toward remediation, and an outline of future updates.
- Update any firewalls and network security to capture evidence that can be used later for forensics.
- Engage the legal team and examine compliance and risks to see if the incident impacts any regulations.
- Contact law enforcement if applicable since the incident may also impact other organizations. Additional intelligence on the incident may help eradicate, identify the scope, or assist with attribution.

Post-incident activities (Recovery and Follow-up actions) include eradication of the security risk, reviewing and reporting on what happened, updating your threat intelligence with new information about what’s good and what’s bad, updating your IR plan with lessons learned from the security incident, and certifying then re-certifying your environment is in fact clear of the threat(s) via a post-incident cybersecurity compromise assessment or security and IT risk assessment.

Recovery

- Eradicate the security risk to ensure the attacker cannot regain access. This includes patching systems, closing network access, and resetting passwords of compromised accounts.

- During the eradication step, create a root cause identification to help determine the attack path used so that security controls can be improved to prevent similar attacks in the future.
- Perform an enterprise-wide vulnerability analysis to determine whether any other vulnerabilities may exist.
- Restore the systems to pre-incident state. Check for data loss and verify that systems integrity, availability, and confidentiality has been regained and that the business is back to normal operations.
- Continue to gather logs, memory dumps, audits, network traffic statistics and disk images. Without proper evidence gathering, digital forensics is limited so a follow-up investigation will not occur.

Follow-Up

- Complete an incident response report and include all areas of the business that were affected by the incident.
- Determine whether management was satisfied with the response and whether the organization needs to invest further in people, training or technology to help improve its security posture.
- Share lessons learned. What went well, what didn't and how can procedures be improved in the future?
- Review, test and update the cybersecurity incident response plan on a regular basis, perhaps annually if possible.
- Conduct a compromise assessment or other security scans on a regular basis to ensure the health of systems, networks and devices.
- Update incident response plans after a department restructure or other major transition.
- Keep all stakeholders informed about the latest trends and new types of data breaches that are happening. Promote the message that "security is everyone's job."

Appendix C – Ransomware Attack Response and Prevention

Ransomware Attack Response Checklist

Step 1: Disconnect Everything

- ☐ Unplug computer from network
- ☐ Turn off any wireless functionality; Wi-Fi, Bluetooth, NFC

Step 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption

- ☐ Mapped or shared drives
- ☐ Mapped or shared folders from other computers
- ☐ Network storage devices of any kind
- ☐ External Hard Drives
- ☐ USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- ☐ Cloud-based storage: DropBox, Google Drive, OneDrive etc.

Step 3: Determine Ransomware Strain

- ☐ What strain/type of ransomware? For example: CyrptoWall, Teslacrypt etc.

Step 4: Determine Response

Ransomware response should be determined by a response team, senior leadership, and legal counsel at a minimum. In many cases, law enforcement may provide addition insight or suggestions. You may also want to call in a ransomware response team to assist with restoration.

Response 1: Restore your Files from Backup

1. Locate your backups
 - a. Ensure all files you need are there
 - b. Verify integrity of backups (i.e., media not reading or corrupted files)
 - c. Check for Shadow Copies if possible (may not be an option on newer ransomware)
 - d. Check for any previous versions of files that may be restored on cloud storage e.g., DropBox, GoogleDrive, OneDrive
2. Remove the ransomware from your infected system
3. Restore your files from backups
4. Determine infection vector and handle

Response 2: Try to Decrypt

1. Determine strain and version of the ransomware if possible
2. Locate a decryptor, there may not be one for newer strains; If successful, continue to next steps...
3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)
4. Decrypt files
5. Determine the infection vector and handle

Response 3: Do Nothing (Lose Files)

1. Remove the ransomware
2. Backup your encrypted files for possible future decryption (optional)

Response 4: Negotiate and/or Pay the Ransom

1. If possible, you may attempt to negotiate a lower ransom and/or longer payment period
2. Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.
3. Obtain payment, likely Bitcoin:
 - a. Locate an exchange you wish to purchase a Bitcoin through (time is of the essence)
 - b. Set up account/wallet and purchase the Bitcoin
4. Re-connect your encrypted computer to the internet
5. Install the TOR browser (optional)
6. Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been setup for this specific ransom case
7. Pay the ransom: Transfer the Bitcoin to the ransom wallet
8. Ensure all devices that have encrypted files are connected to your computer
9. File decryption should begin within 24 hours, but often within just a few hours
10. Determine infection vector and handle

Step 5: Protecting yourself in the Future

- ☐ Implement Ransomware Prevention Checklist to prevent future attacks

Ransomware Prevention Checklist***First Line of Defense: End Users***

- ☐ Implement effective security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.
- ☐ Conduct simulated phishing attacks to inoculate users against current threats.
- ☐ Require multi-factor authentication for all end user accounts, regular and administrative

Second line of Defense: Software

- ☐ Ensure you have and are using a firewall.
- ☐ Implement antispam and/or anti-phishing. This can be done with software or through dedicated hardware.
- ☐ Ensure everyone in your organization is using top notch up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking.
- ☐ Implement software restriction policies on your network to prevent unauthorized applications from running. (optional)
- ☐ Implement a highly disciplined patch procedure that updates any and all applications that have vulnerabilities.

Third Line of Defense: Backups

- ☐ Implement a backup solution: Software based, hardware based, or both.
- ☐ Ensure all possible data you need to access or save is backed up, including mobile/USB storage.

- ☐ Ensure your data is safe, redundant and easily accessible once backed up.
- ☐ Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups.

Appendix C

Physical Security Incident Plan



**Golden Spread
Electric Cooperative, Inc.**

A Touchstone Energy® Cooperative



Emergency Action Plan

Emergency Action Plan ("EAP")

Purpose

[REDACTED]

Administrative Duties

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Name:	Title:
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

Alarms

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Emergency responder:	Telephone number:
Fire Dept.	911
Police Dept.	911
Sheriff Dept.	911
Ambulance	911
Poison Control	1-800-222-1222
Spill Response	1-800-424-8802

Emergency Reporting and Weather Monitoring Procedures

In the Event of an Emergency Requiring Evacuation

[REDACTED]

The fire alarm will be activated or whoever notices the fire will make the appropriate call to 911, which will notify the local fire department either Amarillo FD or Lubbock FD.

Our backup method for reporting emergencies that require evacuation includes the following:

Medical Emergencies

Remain calm

Call 9-1-1

[REDACTED]

First responders will administer first-aid as needed until EMT's arrive.

In the Event of a Tornado Watch





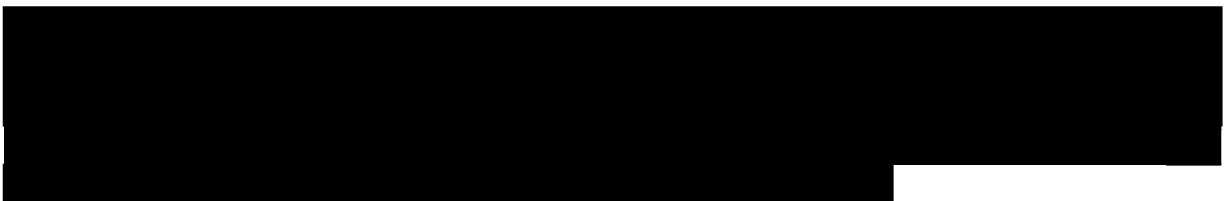
[REDACTED]

[REDACTED]



ACTIVE SHOOTER EVENT

An active shooter is a person or persons who appears to be actively engaged in harming or attempting to kill people in the facility. They may use firearms, other weapons, or improvised explosive devices. Although authorities and the employer are working hard to protect you, situations can arise, and employees may be in danger. In most active shooter cases, warning signs may vary, motivations are different, and there may be no pattern or method for selecting victims.



[REDACTED]

LOCK-DOWN PROCEDURE

[REDACTED]

BOMB THREAT RESPONSE PROCEDURE

[REDACTED]

Evacuation Procedures

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

EVACUATION DUE TO FIRE

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

TORNADOES

[REDACTED]

IF YOU ARE INSIDE:

[REDACTED]

[REDACTED]

EVACUATION:

[REDACTED]

Departmental group:	Designated safe area:

Procedures to Account for Employees

[Redacted]

Name/title:	Department / Location	Shift:

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Responding to a tornado alarm

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan Administrator Duties

[REDACTED]

- [REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Rescue and First Aid

[REDACTED]

Circumstances:	Procedures:
Medical Emergency	Proper PPE - First Aid
Chemical Emergency	Proper PPE and containment

[REDACTED]

Name (or title):	Department / Location	Shift:
------------------	-----------------------	--------

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

Training

- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Appendices

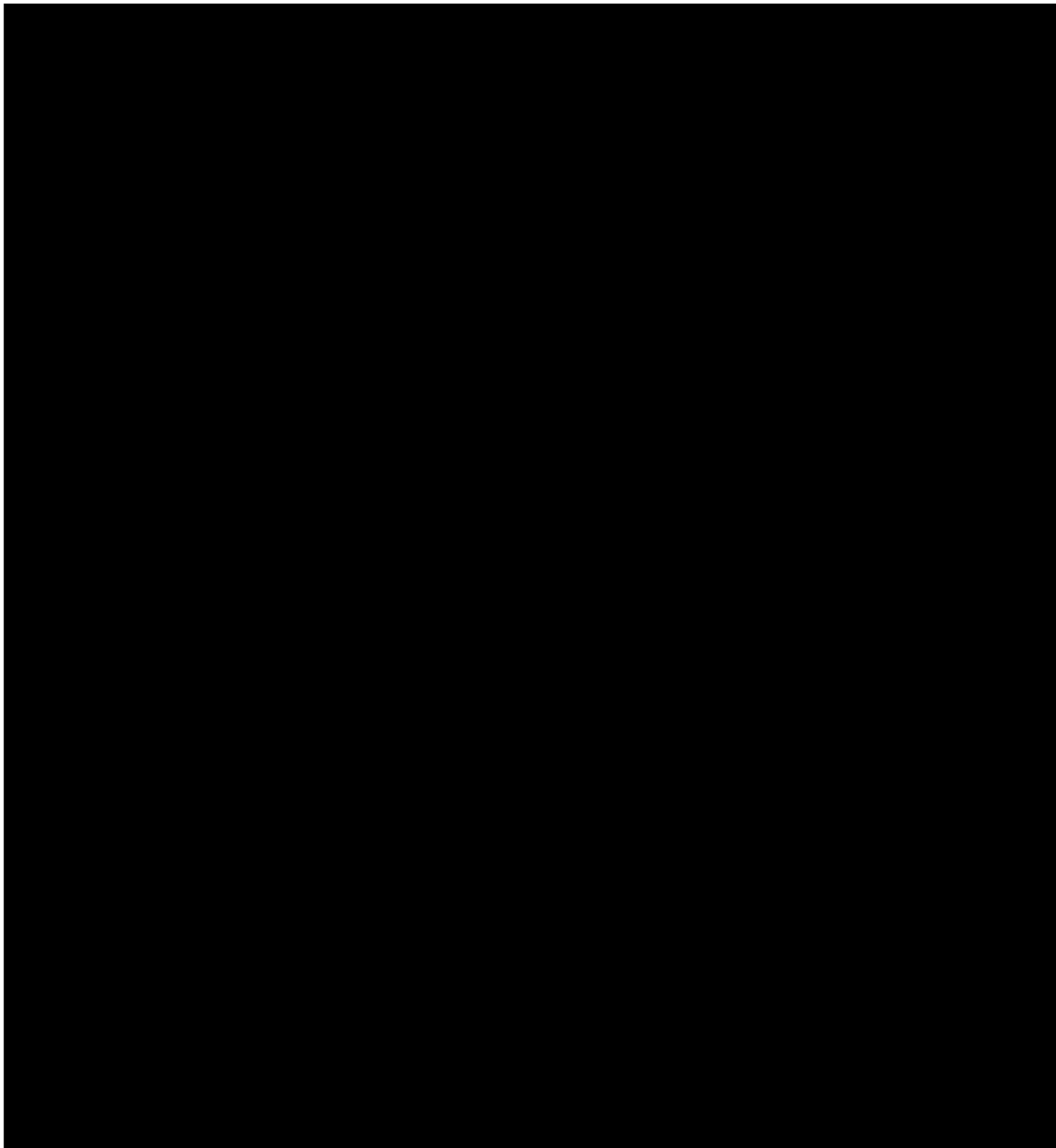
[REDACTED]

[REDACTED]

[REDACTED]

■

EXAMPLE OF AN EVACUATION MAP AND ROLL CALL



Appendix D

Mustang Station Procedures



Mustang Station Operations Manual

Emergency Operating Procedure Major Plant Fire EOP-1

Mustang Station

Denver City, Texas

Rev	Date	Prepared By	Reviewed By	Approved By
2	06-16-2014	PIC Group Inc.	D. Horwath	<i>Carl Brunk</i>
3	04-29-2021	NRG Energy	H. Moreno	M. Goller

This document contains proprietary information of Mustang Station, Inc. and is furnished to its client solely to assist him in the operation of the equipment described herein. This document shall not be reproduced in whole or in part nor shall its contents be disclosed to any third party without the written approval of Mustang Station, [REDACTED]

**Procedure Revision Summary**

1.	Document and Revision Number: Procedure EOP-1
2.	Document Title: Major Plant Fire
3.	Effective Date: 06-16-2014
4.	Document Change:
Rev 0	Initial draft for procedure
Rev 1	Updated Procedure
Rev 2	Reformat Procedure
Rev 3	Replace SPS with Xcel. Minor Format changes
5.	Training Requirements: Required reading for all affected personnel. The precautions to be observed by operating staff personnel during their work within the plant.



TABLE OF CONTENTS

<u>SECTION</u>	<u>TITLE</u>	<u>PAGE</u>
1.0	Initial Conditions	4
2.0	Symptoms/Indications	5
3.0	Possible Causes	5
4.0	Immediate Actions	5
5.0	Supplementary Actions	7



1.0 Initial Conditions

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]



2.0 Symptoms/Indications

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

3.0 Possible Causes

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

4.0 Immediate Actions

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]ment 911.
 - Police 911.



4.0 Immediate Actions, Continued

- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
[REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
[REDACTED]



4.0 Immediate Actions, Continued

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

5.0 Supplementary Actions

- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]

MUSTANG STATION - MAJOR FIRE RESPONSE CHECKLIST

IMMEDIATE ACTIONS

[illegible]



Mustang Station Operations Manual

Emergency Operating Procedure Gas Turbine Trip EOP-2

Mustang Station
Denver City, Texas

Rev	Date	Prepared By	Reviewed By	Approved By
2	06-16-2014	PIC Group Inc.	D. Horwath	<i>Carol Brunko</i>
3	04-29-2021	NRG Energy	H. Moreno	M. Goller

This document contains proprietary information of Mustang Station, Inc. and is furnished to its client solely to assist him in the operation of the equipment described herein. This document shall not be reproduced in whole or in part nor shall its contents be disclosed to any third party without the written approval of Mustang Station, [REDACTED]



Procedure Revision Summary

1.	Document and Revision Number: Procedure EOP-2
2.	Document Title: Gas Turbine Trip
3.	Effective Date: 06-16-2014
4.	Document Change:
Rev 0	Initial draft for procedure
Rev 1	Updated Procedure
Rev 2	Reformatted Procedure
Rev 3	Minor format changes
5.	Training Requirements: Required reading for all affected personnel. The precautions to be observed by operating staff personnel during their work within the plant.



TABLE OF CONTENTS

SECTION	TITLE	PAGE
1.0	Introduction	4
2.0	Symptoms/Indication.....	4
3.0	Possible Causes	4
4.0	Immediate Actions	5
5.0	Supplementary Actions	6



1.0 INTRODUCTION

[REDACTED]

2.0 SYMPTOMS/INDICATION

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

3.0 POSSIBLE CAUSES

[REDACTED]

- | | |
|--------------|--------------|
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |



3.0 POSSIBLE CAUSES, Continued

- | | |
|--------------|--------------|
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |
| ■ [REDACTED] | ■ [REDACTED] |

4.0 IMMEDIATE ACTIONS

- [REDACTED]
[REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



5.0 SUPPLEMENTARY ACTIONS

- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]



Mustang Station Operations Manual

Emergency Operating Procedure Loss of Gas Turbine Lube Oil EOP-3

Mustang Station Denver City, Texas

Rev	Date	Prepared By	Reviewed By	Approved By
2	06-16-2014	PIC Group Inc.	D. Horwath	<i>Carl Brænke</i>
3	04-29-2021	NRG Energy	H. Moreno	M. Goller

This document contains proprietary information of Mustang Station, Inc. and is furnished to its client solely to assist him in the operation of the equipment described herein. This document shall not be reproduced in whole or in part nor shall its contents be disclosed to any third party without the written approval of Mustang Station. [REDACTED]



Procedure Revision Summary

1.	Document and Revision Number: Procedure EOP-3
2.	Document Title: Loss of Gas Turbine Lube Oil
3.	Effective Date: 06-16-2014
4.	Document Change:
Rev 0	Initial draft for procedure
Rev 1	Updated Procedure
Rev 2	Reformat Procedure
Rev 3	Minor Format changes
5.	Training Requirements: Required reading for all affected personnel. The precautions to be observed by operating staff personnel during their work within the plant.



TABLE OF CONTENTS

<u>SECTION</u>	<u>TITLE</u>	<u>PAGE</u>
1.0	Initial Conditions	4
2.0	Symptoms/Indication	4
3.0	Possible Causes	4
4.0	Immediate Actions	4
5.0	Supplementary Actions	5



1.0 Initial Conditions

[REDACTED]

2.0 Symptoms/Indication

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

3.0 Possible Causes

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

4.0 Immediate Actions

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]



4.0 Immediate Actions, Continued

- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
[REDACTED]
[REDACTED]

5.0 Supplementary Actions

- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]



4.0 Supplementary Actions, Continued

- [REDACTED]
[REDACTED]
- [REDACTED]
- [REDACTED]



Mustang Station Operations Manual

Emergency Operating Procedure Steam Turbine Generator Trip EOP-4

Mustang Station Denver City, Texas

Rev	Date	Prepared By	Reviewed By	Approved By
2	06-16-2014	PIC Group Inc.	D. Horwath	<i>Carl Brunk</i>
3	04-29-2021	NRG Energy	H. Moreno	M. Goller

This document contains proprietary information of Mustang Station, Inc. and is furnished to its client solely to assist him in the operation of the equipment described herein. This document shall not be reproduced in whole or in part nor shall its contents be disclosed to any third party without the written approval of Mustang Station.

**Procedure Revision Summary**

1.	Document and Revision Number: Procedure EOP-4
2.	Document Title: Steam Turbine Generator Trip
3.	Effective Date: 06-16-2014
4.	Document Change:
Rev 0	Initial draft for procedure
Rev 1	Updated Procedure
Rev 2	Reformat Procedure
Rev 3	Minor Format Changes
5.	Training Requirements: Required reading for all affected personnel. The precautions to be observed by operating staff personnel during their work within the plant.



TABLE OF CONTENTS

SECTION	TITLE	PAGE
1.0	Introduction	4
2.0	Symptoms/Indication.....	4
3.0	Possible Causes	4
4.0	Immediate Actions	5
5.0	Supplementary Actions	6