

Design Document - Information Security: Incident Response & Reporting

Business Purpose	<p>In the past two years, Alliance insurance company has seen an increase in cyber security incidents by 15%. Due to these incidents, Alliance has seen a loss \$2.3 million over the last two years. If not addressed, member premiums will increase.</p> <p>The purpose of this course is to provide Alliance insurance employees with a list of types of cyber security incidents that can occur in the workplace, a process to report and respond to those security incidents, and a list of contacts to advise when a security incident occurs.</p>
Target Audience	<p>All Alliance insurance employees using computer systems in the office workplace or on a work computer at home</p>
Training Time	<p>20 minutes</p>
Training Recommendation	<p>All Alliance insurance employees have access to company computers & computer systems; therefore, all employees are required to take this training. Due to employees being geographically dispersed, having varied work schedules, and living in different time zones, an e-Learning course is the best form for delivering this training.</p>
Deliverables	<ul style="list-style-type: none"> • 1 e-Learning course <ul style="list-style-type: none"> ○ Developed in Articulate Storyline ○ Includes voice-over narration ○ Includes two knowledge checks: (1) multiple response and (1) drag & drop ○ Final Quiz (5 questions, 80% passing) • Storyboard with script
Learning Objectives	<ul style="list-style-type: none"> • Define cyber security incidents • List the steps to report a security incident • Identify common security incidents • Identify who to contact in case of a security incident
Training Outline	<p>Introduction</p> <ul style="list-style-type: none"> • Welcome • Navigation • Purpose • Learning Objectives <p>Topic: What is a Cyber Security Incident?</p> <ul style="list-style-type: none"> • Define the phrase: cyber security incident • Explain the time sensitivity for the incident • Advise what’s at risk if not addressed • Explain repercussions if not reported • <i>Examples provided:</i>

- Accidentally sending confidential email
- Providing access to unauthorized personnel
- Encountering a security risk that compromises company information and information systems
- Experiencing loss, damage, theft of equipment, media, or documents
- *Knowledge Check: What information is true about a cyber security incident?*
 - Multiple answer response (6 options, 4 are correct)
 - 2 attempts provided

Topic: Reporting a Cyber Security Incident

- Explain when to report
- Reminder: If you see something, say something
 - All incidents need to be reported quickly
 - Report even if you are not sure
- 5 steps will be provided in order to report a cyber security incident:
 - **Step 1 – Stop Everything!**
 - List ALL things employee should NOT do when a cyber security incident occurs
 - **Step 2 – Contact**
 - List of who to contact when cyber security incident occurs
 - **Step 3 – Send mitigating email**
 - Advise who to email
 - Advise what to do with email after incident occurs
 - **Step 4 – Write down information**
 - Explain what to write down when a cyber security incident occurs
 - **Step 5 – Following an incident**
 - Wait for supervisor directions
 - Not using systems until given okay from supervisor
- *Knowledge Check: Drag & Drop*
 - Learner must organize list of steps in correct order
 - 2 attempts

Topic: Who to Contact?

- Section reinforces who to inform when cyber security incident occurs

	<ul style="list-style-type: none"> • Three methods of contact <ul style="list-style-type: none"> ○ Call Company Call Center ○ Advise Supervisor ○ Email same recipients of original email or data spill <p>Assessment</p> <p>Summary</p> <p>Congratulations</p>
<i>Assessment Plan</i>	<p>2 Knowledge Checks</p> <p>Final Assessment</p> <ul style="list-style-type: none"> • 80% passing on e-learning module assessment • Unlimited attempts • 5 questions <ul style="list-style-type: none"> ○ 1 True/False ○ 3 Multiple Choice ○ 1 Drag and Drop
<i>Evaluation of Success</i>	<p>Employees will now be able to:</p> <ul style="list-style-type: none"> • Recognize a cyber security incident. • Follow the 5-step process in reporting a security incident. • Contact appropriate contacts immediately. <p>Alliance insurance will see:</p> <ul style="list-style-type: none"> • A reduction in monetary loss due to cyber security incidents. • Employees dealing with cyber security incidents quickly and efficiently.