LIDMAN LAW, APC
Scott M. Lidman (SBN 199433)
slidman@lidmanlaw.com
Milan Moore (SBN 308095)
mmoore@lidmanlaw.com
Tiara Gose-Hardy (SBN 323823)
tgose@lidmanlaw.com
2155 Campus Drive, Suite 150
El Segundo, California 90245
Tel: (424) 322-4772
Fax: (424) 322-4775

Attorneys for Plaintiffs
FRANCISCO HERNANDEZ, LUCIANO ESQUEDA, CARLOS LOPEZ, and RAMON ALCALA NAVARRO

[*Additional counsel on following page*]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

FRANCISCO HERNANDEZ, LUCIANO ESQUEDA, EFRAIN IBARRA, CARLOS LOPEZ, RAMON ALCALA NAVARRO, as individuals and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOLD POINT TRANSPORTATION, INC., a California corporation; and DOES 1 through 100, inclusive,

Defendants.

Case No.: 21STCV35686

[*Assigned for All Purposes to Hon. William F. Highberger, Dept. SSC-10*]

DECLARATION OF JODEY LAWRENCE OF PHOENIX SETTLEMENT ADMINISTRATORS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY APPROVAL

Date: February 10, 2027
Time: 11:00 a.m.
Dept.: SSC-10

HAINES LAW GROUP, APC
Paul K. Haines (SBN 248226)
phaines@haineslawgroup.com
2155 Campus Drive, Suite 180
El Segundo, California 90245
Tel: (424) 292-2350
Fax: (424) 292-2355

Attorneys for Plaintiff
FRANCISCO HERNANDEZ, LUCIANO ESQUEDA, CARLOS LOPEZ, and RAMON ALCALA NAVARRO

DECLARATION OF JODEY LAWRENCE

I, JODEY LAWRENCE, declare as follows:

1. I have personal knowledge of the facts set forth herein and if called upon to testify, I could and would do so competently under oath.

2. I am employed by Phoenix Settlement Administrators ("Phoenix"), as Vice President of Business Development.

3. I personally have over sixteen years of experience in claims management and administration of class and collective action matters.

4. Phoenix has never had any financial interests in nor affiliation with the parties or counsel in the *Francisco Hernandez, et al. v. Gold Point Transportation, Inc.* matter.

5. Phoenix has extensive experience administering class action matters. Phoenix has administered complex wage and hour, labor and employment, consumer/ product liability, TCPA, FLSA, FACTA, ERISA and PAGA class action matters, thru final approval and distribution. Phoenix has developed a system of quality assurance measures, to ensure the highest quality service is provided in our cases and to class members.

6. Phoenix's Claims Management Group has extensive experiences in all aspects of Notification and Identification of Class Members, Claims Processing, Formulation and Calculation Methodologies, Award Distribution and Taxation, Accounting and Reconciliation.

7. Phoenix has extensive experience in and are experts at all aspects of complex class action matters including; (i) preparing, printing, mailing and tracking privacy notices; (ii) operation of a 24/7/365 multi-lingual call center; (iii) establishing settlement websites; (iv) claims management; (v) USPS processes and systems, third party tracing, including the use of reverse telephone directory services; (v) database management, programming and security protocols; (vii) calculating and issuing settlement payments; (viii) tax management, filings, and account reconciliation; and (ix) final approval.

8. As part of Settlement Notice procedures, Phoenix will run the names of all Settlement Class members through the National Change of Address ("NCOA") database to determine any updated addresses for Settlement Class members. If a Class Notice from the initial

notice mailing is returned as undeliverable, the Settlement Administrator will attempt to obtain a current address for the Settlement Class Member to whom the returned Class Notice had been mailed by undertaking skip tracing. If the Settlement Administrator is successful in obtaining a new address, it will promptly re-mail the Class Notice to the Settlement Class Member. Further, any Class Notices that are returned to the Settlement Administrator with a forwarding address before the Response Deadline shall be promptly re-mailed to the forwarding address affixed thereto.

9. Phoenix has been appointed as a Claims Administrator in both State and Federal Courts.

10. A true and correct copy of Phoenix's Curriculum Vitae is attached hereto as **Exhibit A**

11. Phoenix Settlement Administrators has adequate procedure in place to safeguard the data and funds to be entrusted to it. Phoenix's Technology and Banking groups are directly involved with Management on all issues of Information Security and Settlement Fund transfer, as it pertains to the continuance of business processes, and all risk, vulnerability, security and assessments as it pertains to information. The group, along with internal systems in place, monitor and communicate with Management on a Preventative and comprehensive level, in order to prevent potential Strategic or Compliance Risks. All processing of confidential and personal information is handled and maintained within the organization and therefore all data received is kept within a strict chain of custody internally. All informational assets are classified and assigned based on initial case assessment, client and procedural requirements. The Technology Group handles all higher-level ownership of information and physical peripherals, as well as ownership of direct / indirect assets associated with technology and the continuance of business, Specific Users, Groups or Entities are assigned Shared Ownership or Management Capability based on procedural needs, and security level granted. Phoenix's Phoenix Settlement Administrators Data Center Policies and Procedures is attached hereto as **Exhibit B** and Phoenix Server, Facility and Maintenance Security Protocols and Review is attached hereto as **Exhibit C.**

/ /

12. In addition to high levels of Data Center Policies/Procedures and Facility/Maintenance Security Protocols, Phoenix's conducts semiannual training to maintain additional safeguards such as:

a. Phoenix Settlement Administration Business Continuity Policy

b. Phoenix Settlement Administration Disaster Recovery Plan

c. Phoenix Settlement Administration Incident Response Plan

d. Phoenix Settlement Administration Personal Computer Security Policy

e. Phoenix Settlement Administration Phoenix Data Archiving and Retention Policy

f. Phoenix Settlement Administration Phoenix Personnel Security Policy

g. Phoenix Settlement Administration Risk Assessment

h. Phoenix Settlement Administration Service Provider Risk Assessment

i. Phoenix Settlement Administrator Classification and Access Rights Policy

j. Phoenix Settlement Administrator Password Policy

k. Phoenix Settlement Administrators Certification of Destruction

l. Phoenix Settlement Administrators Security Awareness Training Program

A true a correct copy of the materials described above are attached hereto as **Exhibit D.**

13. Phoenix currently maintains an errors and omissions insurance policy, which includes a data breach provision. A true a correct copy of Phoenix's current policy is attached hereto as **Exhibit E.**

14. Phoenix costs are reasonable and competitive when compared to the industry.

15. Phoenix only employs a certified and/or qualified translator to translate Court-approved Notices for postings on Phoenix's website for dissemination to the Class.

/ /

16. This Administration project has a cost not to exceed $7,950.00, which includes costs associated with mailing the Class Notice in both English and Spanish. A detailed breakdown of Phoenix's cost is attached hereto as **Exhibit F**.

I declare under penalty of perjury under the laws of the United States and state of California that the foregoing is true and correct. Executed on September 23, 2026 at Orange, California.



Jodey Lawrence

EXHIBIT A

PHOENIX
SETTLEMENT ADMINISTRATORS
CLASS ACTION SETTLEMENT SOLUTIONS

1411 N. Batavia, Suite 105 Orange, CA 92867
800-523-5773
www.phoenixclassaction.com

CURRICULUM VITAE

Phoenix Settlement Administrators, PSA Overview

Phoenix Settlement Administrators, PSA, is an emerging, National, Class Action Notification and Claims Administration firm, located in San Diego and Newport Beach California. PSA's core competencies ensure delivery of the highest quality and accuracy to its Clients and Class members. With a combined 28 years of expert experience, PSA,'s Managing Partners, Case Supervisors, Managers and Associates, Data Programming, and Certified Secure Strategic Partners, possess all the qualities that our Clients expect throughout the Noticing and Administration process, to Final Approval. It is our Value Pricing, Efficiency, Experience, Consultative Expertise and Delivery, that has perpetuated PSA, as an emerging leader in Class Action Settlement Administration. Expert PSA staff members are currently managing, Consumer and Product Liability, TCPA, Complex Labor & Employment, FLSA, ERISA and PAGA cases.

PSA has over 100 Attorney & Law Firm Clients, which have entrusted us with the management of their claim's administration, because of the "Boutique" attention every case receives. PSA is value driven on all size cases. large or small, cases receive expert management, secure data custody, neutral communication and a dedicated team. This seamless process maintains superior case continuity to ensure our clients receive timely final approval and conclusion to their actions. Phoenix Settlement Administrators implements its successful C.A.S.E. solutions on all our class action matters.

With 10's of Millions of dollars in award distributions currently under management since our inception, PSA has the ability and strengths to manage all levels of Complex Cases. PSA's Staff "Synergy" is our greatest attribute. It allows our people to work closely together and solve our client's case issues. PSA prides itself as a true "Third Party Administrator" and holds Neutrality as a mantra. Because of this approach, both Defense and Plaintiff Clients, experience fairness, trust and confidence in us, and allows for continued business from both parties. PSA has been appointed Third Party Administrator in State and Federal Courts.

We look forward to working with you on your next Class Action Noticing Campaign or Claims Administration. Let us design a C.A.S.E. solution, which will allow us to showcase the difference you'll experience. Superior Service, Class Savings Value Pricing and Timely Outcomes is why our clients come back to PSA.

PHOENIX
SETTLEMENT ADMINISTRATORS

CLASS ACTION SETTLEMENT SOLUTIONS

Expert Core Services

Initial Planning and Consultative Service on Class Action Cases and Noticing Plans.

State/Nationwide Noticing Expertise: Privacy, Media, Publication, Internet & Email Campaigns.

Attorney General(s) CAFA Notification

Claims Programming, Administration, Processing and Reporting.

24/7/365 Multi-Lingual Call Center Support and Claims Processing

Secure Data Management Environment, Individual Firewalls, Encrypted Data and Storage

Settlement Fund Calculations, Solutions, Award Distribution, Award Reconciliation

Tax Filings: State, Federal, EDD, ETT, FUTA, PAGA Payments

Partial PSA Client List, Defense and Plaintiff

Fisher & Phillips
Gordon & Rees
Paul Plevin Sullivan & Connaughton
Call & Jensen
Drinker Biddle
McKenna Long & Aldridge
Greenberg Traurig
Manning & Kass
Littler Mendelson
Kring & Chung
Orrick Herrington & Sutcliffe
Ogletree Deakins Nash Smoak & Stewart
Perkins Coie
Ross Wersching & Wolcott
Winston & Strawn
Sheppard Mullins
Lewis Brisbois Bisgaard & Smith
Morgan Lewis & Bockius
Paul Hastings
Park & Zheng
Sidley Austin
Higgs Fletcher & Mack
Jackson Lewis
Norton Rose Fulbright

Law Offices of Jonathan Ricasa
Dente Law Firm
Mahoney Law Group
Law Office of Thomas Rutledge
Law Office of Briana Kim
Dychter Law Firm
Garay Law Firm
Olsen Law Offices
Gould & Associates
Cohelan, Khoury & Singer
Ridout, Lyon & Ottoson
Carter Law Firm
Law Office of Justian Jusuf
The Phelps Law Group
The Emilio Law Group
Zeldes, Haeggquist & Eck
Markham Law Firm
Arias Ozzello & Gignac
David Yeremian & Associates
Aegis Law Firm
Rukin Hyland Doria & Tindall
Malk Law Firm
Spiro Law Corp
Levine Law Group, APC

EXHIBIT B



Phoenix Settlement Administrators Data Center Policies and Procedures

I. Overview:

Phoenix Settlement Administrators data center policies and procedures are put in place to protect all equipment located within the data center. These steps are put in place by senior Phoenix directors. Phoenix Settlement Administrators main intent and highest level of importance is to keep data safe and secure while behind our doors. Employees and customers working outside of the set policies and procedures are subject to termination, legal action, or sever reprimand.

II. Base Guidelines

The Data Center is a restricted area within the Phoenix Settlement Administrators building. The Data Center mandates a much greater level of security. Only those individuals who are expressly authorized to do so by Senior Management may enter this area. Access privileges will only be granted to individuals who have a legitimate business need to be in the data center. All Phoenix Settlement Administrators staff working in the Data Center are required to familiarize themselves thoroughly with this document. The only exception allowed to the Data Center Security Policies and Practices is temporary suspension of these rules if it becomes necessary to provide emergency access to medical, fire and/or police officials.

III. Levels of Access to the Data Center

There are three “Levels of Access” to the Data Center - Controlling Access, Escorted Access, and Unescorted Access.

a. Controlling Access is given to people who have free access authority into the Data Center. Controlling Access is granted to Phoenix Core staff whose job responsibilities require that they have access to the area. These individuals also have the authority to grant temporary access to the Data Center and to enable others to enter and leave the Data Center. People with Controlling Access are responsible for the security of the area, and for any individuals that they allow into the Data Center. If a person with Controlling Access allows Escorted Access to an individual, the person granting access is responsible for escorting the individual granted access and seeing to it they sign in and out. If needed, these duties can be handed-off to one of the Phoenix Operators on duty in the Data Center.

b. Escorted Access is closely monitored access given to people who have a legitimate business need for infrequent access to the Data Center. “Infrequent access” is generally defined as access required for less than 15 days per year. Individuals with Escorted Access will not be issued keys or be granted access via key code combination. A person given Escorted Access to the area must sign in and out under the direct supervision of a person with Controlling Access, must provide positive identification upon demand, and must leave the area when requested to do so. Individuals allowed Escorted Access will be placed on the Phoenix Operations Authorized Access List. A person with Escorted Access to the area must not allow any other person to enter or leave the area.

c. Unescorted Access is granted to a person who does not qualify for Controlling Access but has a legitimate business reason for unsupervised access to the Data Center. Individuals with Unescorted Access to the Data Center will be granted access to the area through a Phoenix core employee with controlling access. Unescorted Access personnel cannot authorize others to be granted unsupervised access to the Data Center. Customers who are given Unescorted Access may NOT escort anyone into the Data Center without approval from personnel with Controlling Access authority. ALL visitors must sign in when entering and sign out when leaving the Data Center.

d. Data Center Doors

All doors to the Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:

- Allow officially approved and logged entrance and exit of authorized individuals;
- Permit the transfer of supplies/equipment as directly supervised by a person with Controlling Access to the area;

e. Security System and Keys

It is the policy of Senior Management not to issue keys to the Data Center for routine access purposes. Requests for exceptions to this policy will be considered on a discretionary, case-by-case basis. If Senior Management issues a key to an individual, the individual may not share, loan or copy the key. All keys are marked “Do Not Duplicate” preventing a legal copy from being made. Only those granted Controlling Access can request and be issued keys. Under no circumstances may an individual attempt to bypass the Locking system to gain access for them or permit access to another individual.

f. Periodic Review and Termination/Revocation of Access

Periodic (at least annual) reviews will be performed of those with any level of access to the Data Center. Senior Management will perform these reviews. If an individual no longer requires Data Center access, it will be revoked. The Joint Management Team will also perform periodic (at least annual) reviews of those with keys to the Data Center. If an individual's needs no longer justify a key, it will be collected. Procedures for terminating or revoking Data Center access include:

- Changing Key
- Collecting Key

g. Access Control Log

The Data Center Access Control Log must be properly maintained at all times. The Log is maintained by Operations staff. All individuals with Controlling Access to the Data Center are responsible for maintaining this log. The following procedures must be followed:

- Each time an individual with Escorted Access to the Data Center is admitted to the area, he must properly log in on the Access Control Log at the time of entrance. The person admitting the visitor must countersign and fill out the appropriate section of the form.
- Each time an individual with Escorted Access leaves the area, he must properly log out on the Access Control Log at the time he leaves (even if only for a short time). The person with Controlling Access to the area who allows the visitor to leave must fill out the "Log Out" section of the Access Control Log.

h. Exception Reporting

All infractions of the Data Center Physical Security Policies and Procedures shall be reported to the Joint Management Team. If warranted (e.g.: emergency, imminent danger, etc.) the police will be notified immediately. If an unauthorized individual is found in the Data Center it is be reported immediately to Senior Management. They will determine if the police should be contacted. The unauthorized individual should be escorted from the Data Center and a full written report should be immediately submitted to Senior Management. Any attempt to forcibly or improperly enter of the Data Center should be immediately reported to the police, who should deal with the situation. The person present with controlling access will report the incident in writing to Senior Management. Individuals with Controlling Access to the area are to monitor the area and remove any individual who appears to be compromising either the security of the area or its activities, or who is disrupting operation.

i. Escalation

Senior Management has overall responsibility for the administration of these policies and procedures. Issues that Senior Management is unable to resolve will be escalated to the Phoenix Settlement Administrators executives.

IV. General Data Center Operations Policies

a. General Safety Policy

All individuals in the Data Center must conduct their work in observance with all applicable (ie: state, federal) policies related to safety.

b. General Cleanliness Policy

The Data Center must be kept extremely clean. All individuals in the Data Center are expected to maintain cleanliness. Tools must be replaced to their rightful place. Food and drink are not allowed in the Data Center.

c. Policies for Data Center Equipment Deliveries/Pick-Up

A log is maintained by Phoenix that identifies and verifies all equipment that is brought into or removed from the Data Center. The Phoenix Operations manager will be responsible for logging all equipment that is scheduled to arrive or be picked up from the Data Center. Any customer that is planning to have equipment delivered to or picked up from the Data Center should contact Phoenix Operations and provide details to Phoenix Operations in advance of delivery/pick-up. Please provide Operations with the following information for the equipment log:

For the delivery of equipment:

- Expected day of delivery;
- Vendor name and description of the equipment;
- Person to be contacted when the equipment arrives For the pick-up of equipment;
- Expected day the equipment will be picked up;
- Vendor name and the description and location of the equipment to be picked up;

V. Rules:

Those granted data center access must abide by the following rules:

- Access must not be used to allow any unauthorized person into the data center.
- Individual that has access MUST formally log in and out ALL visitors that are accompanying them into the data center.
- Individuals with access privilege must abide by all policies and procedures as described in the Phoenix Settlement Administrators Data Center Access Policies and Procedures document.
- Violating these rules may result in the revoking of access to the Data Center. The Operations Manager will facilitate the Data Center standards and procedures review process for all prospective data center tenants.

EXHIBIT C

PHOENIX
SETTLEMENT ADMINISTRATORS
CLASS ACTION SETTLEMENT SOLUTIONS
1411 N. Batavia Street, Suite 105, Orange, Ca. 92867 Telephone (800) 523-5773

Phoenix Server, Facility and Maintenance Security Protocols and Review

Phoenix, Settlement Administrators, Inc. Data Security and Server Annual Review
Overview:
As a matter of security enhancement and maintenance, Phoenix, Inc. performs a periodic audit of all data servers integral in maintaining security, systems efficiencies, safety, redundancy, and equipment capacity. The following document details all checks done to ensure proper attention in each area.

Server Room and Facility Security:

Trilogy Key Code Combination Locks (3 Locks in Facility "DC1 / DC2 / LBY1")
-code changed, quarterly (Yes)
-internal battery replaced, yearly (Yes)
-manual override key secured in office safe (Yes)
(Internal Maintenance, Operations Director Julie Keller)

Axis Security Camera Network (4 Cameras in Facility "Lobby / Outside Server Room / Inside Server Room / Rear & Front Door")
-change password on main camera server, quarterly (Yes)
-check each camera video display, daily (Yes)
-check camera server for 45 day retention of video, quarterly (Yes)
-check cameras for proper motion detection, weekly (Yes)
-clean outdoor camera lenses, bi-yearly (Yes)
(External Maintenance, Secure View, Robby Caldwell)

Securitron External Door Locking System (Lock System for Facility "Doors")
-code changed, bi-yearly (Yes)
-internal backup battery replaced, yearly (Yes)
-locking door magnets checked for proper locking (Yes)
(Internal Maintenance, Production Manager – David Voyen)

Server Room Alarm System
-individual combination for each authorized employee (Yes)
-codes changes, bi-yearly (Yes)
-door sensors check, monthly (Yes)
-motion detector check, quarterly (Yes)
-audible alarm check, bi-yearly (Yes)
-backup battery replaced, yearly (Yes)
(Internal Maintenance, Production Manager –David Voyen)

Data Center Log
-cross reference visitor log entry with video surveillance, monthly (Yes)
-cross reference equipment removal forms with video surveillance, monthly (Yes)
(Internal Maintenance, Operations Director – Julie Keller)

Data Center Network Security:

Microtik Edge Router
-quarterly password change
-firmware upgrade performed as released
(Internal Maintenance, Senior Engineer – Mill Systems)

Intrusion Detection System
-firmware upgrade performed as released
(Internal Maintenance, Senior Engineer – Mill Systems)

Policies and Procedures
-staff review, bi-yearly
-educational review, bi-yearly
-Terminal and Log-In passwords changed, quarterly
-Updated Records of Required Password & Log-In required Changes, quarterly
(Internal Maintenance, VP Operations – Melissa Meade & Michelle Reynolds, Esq)

Server Room Infrastructure Maintenance:

Powerware 80KVA UPS
-preventative maintenance PM check, annual (Yes)
-monthly battery test (Yes)
-visual inspection (Yes)
(Contracted Maintenance)

Kohler 15REOZK 0-100KW Generator Set
-30 minute operation/inspection every 30 days (Yes)
-emergency power transfer drill, annual (Yes)
-fluid check every 30 days (Yes)
-annual inspection and complete fluid change (Yes)
(Contracted Maintenance, Tier 4 Generators, Tustin- Ron Aglio)

Building Fire Suppression System
-annual inspection (Yes)
-control panel visual inspection (Yes)
(Contracted Maintenance, Jon Rash)

Handheld Halon Bottles in Data Center
-annual inspection and pressure test (Yes)
(Contracted Maintenance, Hendricks Fire)

HVAC Building Cooling Systems
-inspection of all units, annual (Yes)
-filter replacement, quarterly (Yes)

EXHIBIT D

PHOENIX BUSINESS CONTINUITY POLICY

Table Of Contents

1 Purpose - Business Continuity Management 3

2 Policy Statement 3

2.1 Business Impact Analysis 3
2.2 Risk mitigation 3
2.3 Business continuity strategy 3
2.4 Business Continuity Plan 3
2.5 Disaster Recovery Plan 4
2.6 DR Document 4
2.7 Testing 5
2.8 Updating your BCP and DRP 5

1 Purpose - Business Continuity Management

In accordance with industry 'best practices' and to comply with numerous compliance regulations, Phoenix has implemented various Information Security policies and procedures in order to protect the confidentiality, integrity and availability (CIA) of their critical client data, their computing resources, and their business interests. This document provides describes the Business Continuity Management procedures to be performed by the IT staff at Phoenix.

2 Policy Statement

2.1 Business Impact Analysis

Before a Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP) is created, a Business Impact Analysis (BIA) must be performed on each business unit's systems and processes.
Guidelines for this can be found in the, "Phoenix's Risk Assessment Planning Guide for Information Technology Systems".
Things to consider:

- A determination the maximum time of not having the service(s) provided by the system that can be tolerated.

An identification of all of the threats to the system such as:

- Program or Data Failure.
- Hardware Failure.
- Electrical Power Failure.
- Fire.
- Natural disasters

2.2 Risk mitigation

Following the BIA, appropriate controls should be considered for implementation in order to decrease the risk to an acceptable level.

The business process owner should discuss all risk mitigation options with Management before the strategy is developed.

2.3 Business continuity strategy

Business process owner and Management should then develop a business continuity strategy consistent with business objectives. Emphasis should be on restoring services within the acceptable time.

- BCP recovery strategies should include input from all relevant business units. This ensures that there is ownership of the BCP strategy by the business units.
- Assess all the risks associated with the strategy you have adopted.
- Business owners must weigh their tolerance for downtime when selecting a recovery strategy.
- Once the strategy is determined, develop the BCP.

2.4 Business Continuity Plan

All COMPANY locations must create high-level BCP's (often non-IT system specific, business recovery). BCP's should include manual processes where possible and should be developed in conjunction with Business Process Owners, not IT personnel. Individuals must be assigned to execute each component of the plan.

2.5 Disaster Recovery Plan

DRP can be included with the BCP and will often involve IT specific recovery. Business Process owners and IT personnel must work together to create the DRP. All IT systems should be considered during the development of the plan. Individuals must be assigned to execute each component of the plan.

For example, the following areas should be included in the plan :

- Data backup – media/content must be sent offsite.
- Documentation backup – all hard copies and soft copies
- Archived data – may include removable and internal media
- Facilities backup – for example: backup generator, UPS.
- Business resumption team training – during disaster
- Critical applications
- Alternate processing procedures – for example manual procedures.

2.6 DR Document

Your DR Plan must include a DR document. This is what you will use during an actual disaster and auditors will require it.

This is how the document should be structured:

Mitigation

- *Identify Recovery Components (the scope of the plan)*
- *Perform an Operational Analysis – to ensure current operational flaws are not replicated in emergency mode so you must review the current strategy*
- *Perform a Disaster Risk Analysis*

Examples to look for are:

- *Electronic security*
- *Viruses*
- *Hardware failure*
- *Fire*
- *Power outages*
- *Physical security*

Preparation Mode

Focus on documenting existing systems, network configurations, hardware, applications and assigned personnel.
This answers the question of WHAT needs to be recovered, WHEN (prioritized), HOW and by WHOM.

- *Document Systems and Applications*
- *Perform a (Risk) Tolerance Analysis*
- *Prioritize Recovery*
- *Create Organizational Chart*
- *Create a Contact List (print and distribute)*
- *Put in place a DR Team*
- *Assign Roles and Responsibilities*
- *Review the Plan*
- *Make necessary policy changes to align with the plan*
- *Test the Plan*
- *Implement the Plan*
- *Perform routine Plan Maintenance*

Response Mode

- *Conduct the appropriate actions in the Event of an Emergency – evaluate the problem before engaging Recovery Mode.*

Recovery Mode

- *Execute the plan*

2.7 Testing

Must be tested at least annually where possible.

2.8 Updating your BCP and DRP

Must review annually and updated if.

Phoenix Settlement Administration

Disaster Recovery Plan

Millennium Systems

Last reviewed & tested - 24/07/2018

.

0

Introductions
- Plan scope
- Service RPO and RTO targets
- Backup strategy
- Testing schedule
- Plan review
- Revision history

Roles and responsibilities
- Internal contacts
- External contacts

Incident response

DR procedures

Introduction

This document details the policies and procedures of Phoenix Settlement Administration in the event of a disruption to critical IT services or damage to IT equipment or data. These processes will ensure that those assets are recoverable to the right level and within the right timeframe to deliver a return to normal operations, with minimal impact on the business.

Plan scope

- Local facility
- Data center

Service RPO and RTO targets

IT service	Scenario	RPO	RTO	Priority
Shared Files	Server failure	24 hours	4 hours	High
Email	Server failure	24 hours	8 hours	High
RDS	Server failure	24 hours	8 hours	High
VPN	Router failure	24 hours	8 hours	High

Backup strategy

IT service	Backup location	Backup frequency
Offsite backup	Offsite	Daily
Local Backup	Data Center	Daily

Testing schedule

- The DR plan will be tested in its entirety once every 3 months
- Recovery process for IT service will be tested once every 3 months

Plan review

- The DR plan itself will be formally reviewed once every 3 months and in response to regular testing

Revision history

Version	Date	Revision details
1.0	1/17/2018	
1.1	7/24/2018	Added DR Procedures

Roles and responsibilities

The following individuals are to assume responsibility for restoring IT services when the DR plan is activated:

Internal contacts

Name	Job role	Contact details	DR process owned
Melissa Meade	VP of Operations	(949) 331-0865	None

External contacts

Name	Organisation	Contact details	DR process owned
Millennium Systems	Millennium Systems	(949) 252-8772	Disaster recovery

Incident response

The DR plan is to be activated when one or more of the following criteria are met:

- Loss of data, connectivity, and hardware failure.

The person discovering the incident must notify the following DR stakeholders, who collectively assume responsibility for deciding which - if any - aspects of the DR plan should be implemented, and for establishing communication with employees, management, partners and customers.

- Melissa Meade
- Millennium Systems

DR procedures

Depending on the incident, and on the number and nature of the IT services affected, one or more of the following DR procedures may be activated by the DR team:

DR plan for loss of data

Scenario	Lost data discovered on the server
Possible causes	Data corruption, hardware failure
IT services and data at risk	Shared files
Impact	Lost data

Plan of action	● Identify issue, coordinate initial response (Melissa Meade) ● Evaluate damage (Melissa Meade) ● Contact Millennium Systems (Melissa Meade) ● Establish data recovery targets and timeframes (Millennium Systems) ● Recover data from local or offsite backup (Millennium Systems) ● Verify restored data (Melissa Meade)

Key contacts	● Melissa Meade (VP of Operation) ● Millennium Systems

DR plan for scenario loss of connectivity

Scenario	Connectivity is lost to the servers
Possible causes	Internet connectivity issues or router issues
IT services and data at risk	Shared Files, RDS, Email, VPN
Impact	Lost productivity

Plan of action	● Identify issue, coordinate initial response (Melissa Meade) ● Evaluate damage (Melissa Meade) ● Contact Millennium Systems (Melissa Meade) ● Contact Internet service provider for Internet connectivity issues. (Millennium Systems) ● Replace or resolve router issues (Millennium Systems)

Key contacts	● Melissa Meade (VP of Operation) ● Millennium Systems

DR plan for scenario hardware failure

Scenario	Hardware has failed
Possible causes	Hardware failure on the servers
IT services and data at risk	Shared Files, RDS, Email
Impact	Lost productivity

Plan of action	● Identify issue, coordinate initial response (Melissa Meade) ● Evaluate damage (Melissa Meade) ● Contact Millennium Systems (Melissa Meade) ● Replace hardware and restore data (Millennium Systems)

Key contacts	● Melissa Meade (VP of Operation) ● Millennium Systems

Incident Response Plan

Prepare

In preparing for security incidents several items need to be addressed.

- Incident handling team should include security officers, system analysts and human resources personnel
- End users and analysts should be trained at an appropriate level. Login banner and warning messages should be posted.
- Contact information is included as an appendix to this document and should be available in hard copy for:
    - personnel that might assist in handling an incident
    - key partners who may need to be notified
    - business owners to make key business decisions
    - outside support analysts with security expertise

- Backups should be taken and tested!
- Supplies to assist the team in the event of an incident (sometimes referred to a jump bag)
    - An empty notebook (Thorough documentation should be done throughout an incident to include hand written notes in a fresh notebook.)
    - Boot CDs to analyze hard drives and recover passwords

Identify

Awareness that a security incident has occurred can originate from different sources such as technical people, end users or even clients.

Best practices suggests to declare that an incident has occurred when security officers' sense that an adverse risk to the company exists and then assemble the team and implement the plan. It is also suggested to early on have multiple people involved, to save all key system files or records such as log files and start detailed documentation as soon as possible.

Ultimately business owners need to be involved in many security incidents to decide what are the goals in handling a particular incident, such as immediate business recovery or forensic examination.

Contain

Following basic procedures can contain many incidents. Specific procedures will frequently depend on the nature of the incident, as well as the direction of the business owner. Remember that a compromised machine might not present valid data! Basic steps to consider include:

- Obtain and analyze as much system information as possible including key files and possibly a backup of the compromised machine for later forensic analysis.
- Powering off a machine might lose data and evidence. Preferably disconnecting the LAN cable facilitates containment and forensic activity. (Putting the computer on a separate network with a network analyzer might help analyzing network activity)

- If one machine has been exploited others might be vulnerable. Actions that might need to be taken on a large scale might include:
    - Download security patches from vendors
    - Update antivirus signatures
    - Close firewall ports
    - Disable compromised accounts
    - Run vulnerability analyzers to see where other vulnerable hosts are
    - Change passwords as appropriate

Eradicate

To eradicate the problem specific procedures will frequently depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Boot CDs should be used to access data on compromised machines. (Rootkits installed on compromised machines might affect basic system level utilities and discourage use of a compromised host)
- If machines OS has been compromised it needs to be rebuilt using hardened machines on appropriate platforms
- Test any backups prior to restore and monitor for a new incident.
- Document everything.

Recover

The recovery phase's goal is to return safely to production. Once again specific actions might depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Retest the system preferably with a variety of end users.
- Consider timing of the return to production.
- Discuss customer notification and their concerns
- Continue to monitor for security incidents

Review

This phase is to allow Phoenix to better handle future security incidents. A final report should be written describing the incident and how it was handled using the Incident reporting form. Suggestions for handling future incidents and reworking this document should be included in this report.

Contact information

1. Personnel that might assist in handling an incident:
   Melissa A. Meade
   Vice President of Operations
   Direct: 949.331.0865
   Email: melissa@phoenixclassaction.com

2. Key partners who may need to be notified:
   Michael E. Moore
   President and Managing Partner
   Direct: 949.331.0131
   Email: mike@phoenixclassaction.com

3. Business owners to make key business decisions
   Michael E. Moore
   President and Managing Partner
   Direct: 949.331.0131
   Email: mike@phoenixclassaction.com

4. Outside support analysts with security expertise
   Eric Dee: IT

Additional service provider contacts

PERSONAL COMPUTER SECURITY POLICY

Table of Contents

Purpose.....**Error! Bookmark not defined.**
Scope.....**Error! Bookmark not defined.**
Policy .....**Error! Bookmark not defined.**
Violations..... 1
Definitions..... 5
References.....**Error! Bookmark not defined.**
Related Documents .....**Error! Bookmark not defined.**
Approval and Ownership .....**Error! Bookmark not defined.**
Revision History .....**Error! Bookmark not defined.**

PURPOSE

This policy defines the information security instructions applicable to all workers who use Phoenix personal computers, including Macintoshes, workstations, portable computers, handheld computers, personal digital assistants, and similar computers dedicated to a single user's activity.

SCOPE

This policy applies to all Phoenix computer systems and facilities, including those managed for Phoenix customers. This policy applies to all employees, partners and third-parties with access to Phoenix information assets.

POLICY

Business Use of Systems

Business Use Only - In general, Phoenix computer and communication systems are intended to be used for business purposes only. Incidental personal use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, does not preempt any business activity, and does not cause distress, legal problems, or morale problems for other workers.

Offensive Content - Offensive material that might cast Phoenix in a bad light, including sexist, racist, violent, or other content, is strictly forbidden from all Phoenix personal computers.

Configuration Control

Approved Software Only - Phoenix has a standard list of permissible software packages that users can run on their personal computers [a link to an intranet-posted personal computer configuration standard could be provided here]. Workers must not install other software packages on personal computers without obtaining advance permission from the Information Systems department. Unapproved software may be removed without advance notice to the involved worker.

Prohibited Software Installation - Workers must not permit automatic software installation routines to be run on Phoenix personal computers unless these routines have been approved by the Information Systems Department.

Changes To Operating System Configurations - Workers must not change operating system configurations, upgrade existing operating systems, or install new operating systems on any Company X-supplied computer hardware.

Changes To Hardware - Computer equipment supplied by Phoenix must not be altered or added to in any way without the prior knowledge of and authorization from the Information Systems department.

Access Control

Access Control Package - All Phoenix personal computers must run an access control package approved by the Information Security department. Typically these packages require a fixed password at the time a personal computer is booted and again after a certain period of no activity.

Unattended Active Sessions - Users must not leave their personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

Session Timeout - Users must set the time frame for this period of no activity, at which point the contents of the screen are obscured, to 15 minutes or less. If sensitive information resides on a personal computer, the screen must immediately be protected with this access control package, or the machine turned off, whenever a worker leaves the location where the personal computer is in use.

Choice Of Passwords - The user-chosen passwords employed by access control software packages, and the keys employed by encryption packages, must be at least eight (8) characters in length and conform to the existing Phoenix password construction standards. (Example: These passwords and keys must be difficult to guess. Words in a dictionary, derivatives of user IDs, and common character sequences such as “123456” must not be employed. Personal details such as spouse’s name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords and keys must not be any part of speech including, proper names, geographical locations, common acronyms, and slang.)

Storage Of Passwords - Workers must maintain exclusive control of their personal passwords. They must not share them with others at any time. Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access controls, or in any other locations where unauthorized persons might discover them.

Viruses

Virus Program Installed - All personal computers must continuously run the current version of virus detection package approved by the Information Security department. The current version of this virus package must be automatically downloaded to each personal computer when the machine is connected to the Phoenix internal network.

External Storage Checking - Externally-supplied CD-ROMs, and other removable storage media must not be used unless they have been checked for viruses.

Eradicating Viruses - Workers must not attempt to eradicate a virus without expert assistance. If workers suspect infection by a virus, they must immediately stop using the involved computer, physically disconnect from all networks, and call the Information Systems department Help Desk.

Information Backup

Archival Copies - All personal computer software that is not standard Phoenix software must be copied prior to its initial usage, and such copies must be stored in a safe and secure location. These master copies, perhaps the media issued by the vendor, must not be used for ordinary business activities, but must be reserved for recovery from virus infections, hard disk crashes, and other computer problems.

License Documentation - Documentation about the licenses for such software must be retained to get technical support, qualify for upgrade discounts, and verify the legal validity of the licenses.

Periodic Backup - All sensitive, valuable, or critical information resident on Phoenix computer systems must be periodically backed up. Such backup processes must be performed at least weekly. Department managers must verify that proper backups are being made on all personal computers used for production business activities.

Manual Backups - Unless automatic backup systems are known to be operational, all end users are responsible for making at least one current backup copy of sensitive, critical, or valuable files stored on local disk. These separate backup copies should be made each time that a significant number of changes are saved.

Backup Storage - User-generated backups must be periodically stored off-site in a physically secure location. Selected files from backups must be periodically restored to demonstrate the effectiveness of every backup process.

Copyright Protection - Making unauthorized copies of licensed and copyrighted software, even if for “evaluation” purposes, is forbidden. Phoenix permits reproduction of copyrighted materials only to the extent legally considered fair use or with the permission of the author or Owner. If workers have any questions about the relevance of copyright laws, they must contact corporate legal counsel. Unless they receive information to the contrary, workers must assume that software and other materials are copyrighted.

Networking and Connectivity

Modems - Modems inside or attached to Phoenix office desktop personal computers are not permitted.

Inbound Internet - Inbound Internet connections to Phoenix personal computers are forbidden unless these connections employ an approved virtual private network (VPN) software package approved by the Information Security department. These VPN systems must employ both user authentication features with at least fixed passwords and data interception prevention features, such as encryption.

Downloading Sensitive Information - Sensitive Phoenix information may be downloaded from a multi-user system to a personal computer only if a clear business need exists, adequate controls to protect the information are currently installed on the involved personal computer, and advance

permission from the information Owner has been obtained. This policy is not intended to cover electronic mail or memos, but does apply to databases, master files, and other information stored on mainframes, minicomputers, servers, and other multi-user machines.

Establishing Networks - Workers must not establish electronic bulletin boards, local area networks, modem connections to existing internal networks, Internet commerce systems, or other multi-user systems for communicating information without the specific approval of the Information Security department.

Automatic Device Synchronization - Systems that automatically exchange data between devices, such as a personal digital assistant and a personal computer, must not be enabled unless the systems have been evaluated and approved by the Information Security department.

Physical Security

Positioning Display Screens - The display screens for all personal computers used to handle sensitive or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas. Care must also be taken to position keyboards so that unauthorized persons cannot readily see workers enter passwords, encryption keys, and other security-related parameters.

Locking Sensitive Information - When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.

Preventing Equipment Theft - All office desktop personal computers except portables must be physically secured to desks with approved devices such as locking wires or plates that bolt the equipment to furniture.

Equipment Identification - All personal computer equipment must be marked with visible identification information that clearly indicates it is Phoenix property. Periodic physical inventories must be completed to track the movement of personal computers and related equipment.

Custodians For Equipment - The primary user of a personal computer is considered a Custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a Custodian must promptly inform the involved department manager. With the exception of portable machines, personal computer equipment must not be moved or relocated without the knowledge and approval of the involved department manager.

Use Of Personal Equipment - Workers must not bring their own computers, computer peripherals, or computer software into Phoenix facilities without prior authorization from their department head. Workers must not use their own personal computers for production Phoenix business unless these systems have been evaluated and approved by the Information Security department.

Property Pass - Personal computers, portable computers and related information systems equipment must not leave Phoenix offices unless accompanied by a property pass signed by a department manager.

Environmental Considerations - All personal computers in Phoenix offices must use surge suppressors. Those personal computers running production applications must also have uninterruptible power systems approved by the Information Security department.

Management

Browsing - Workers must not browse through Phoenix computer systems or networks. Steps taken by workers to legitimately locate information needed to perform their job are not considered browsing. Use of the Phoenix intranet is not considered browsing.

Tools To Compromise Systems Security - Unless specifically authorized by the Information Security department, Phoenix workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

Reporting Problems - Users must promptly report all information security alerts, warnings, and suspected vulnerabilities to the Information Systems Help Desk. Users must not use Phoenix systems to forward such information to other users, whether the other users are internal or external to Company X.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Phoenix reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Phoenix does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Phoenix reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

DEFINITIONS

Confidential Information (Sensitive Information) – Any Phoenix information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Phoenix from a third party under a non-disclosure agreement.

Electronic Messaging System – Any device or application that will provide the capability of exchanging digital communication between two or more parties. Examples are electronic messaging, instant messaging, and text messaging.

Information Asset – Any Phoenix data in any form, and the equipment used to manage, process, or store Phoenix data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Objectionable Information or Material – Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected by national or international, federal, regional, provincial, state, or local laws.

Partner – Any non-employee of Phoenix who is contractually bound to provide some form of service to Company X.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

User - Any Phoenix employee or partner who has been authorized to access any Phoenix electronic information resource.

PHOENIX DATA ARCHIVING AND RETENTION POLICY

Table Of Contents

1 Purpose 3

2 Policy Statement 3

2.1 General Policy 3
2.2 Phoenix Management's responsibilities 3
2.3 Phoenix IT's responsibilities 4
2.4 Data classification 4
2.4.1 Administrative Correspondence 4
2.4.2 Fiscal Correspondence 4
2.4.3 General Correspondence 4
2.4.4 Ephemeral Correspondence 4
2.4.5 Customer Sensitive or Confidential Information 4
2.5 Record Retention Schedule 5
2.6 Policy Suspension 5
2.7 Policy Non-Compliance 5

1 Purpose

In accordance with industry 'best practices' and to comply with numerous compliance regulations, Phoenix has implemented various Information Security policies and procedures in order to protect the confidentiality, integrity and availability (CIA) of their critical client data, their computing resources, and their business interests. This document provides describes the data archiving and retention policies and procedures to be performed by the IT staff at Phoenix.

2 Policy Statement

2.1 General Policy

Any data deemed a "***business record***" shall be archived and retained for a specified period of time. A business record is any print or electronic document created and maintained in the ordinary course of business. However, not every data constitutes a business record that must be kept. Data and any of its attachments should be retained if it documents business activities that have evidentiary or reference value, or it is the sole copy of the information. This includes, for example, job offers, contract negotiations where final pricing is set, or a policy memo. It does not include, for example, in-progress drafts, discussions, or negotiations; received copies of policy memos where an original already exists; or non-business correspondence.

Any data that is required by law to be stored for legal reviews and/or audits will also be archived and retained for as long as the law demands. These messages will also be disposed of in accordance with any regulations governing Phoenix and the industry in which it resides.

2.2 Phoenix Management's responsibilities

The procedures for archiving and retaining electronic data must be compliant with the local, federal, and industry laws, regulations, and directives governing the country, state or municipality where each Phoenix office is located.

Phoenix Management is responsible for being aware of, listing and describing the local, federal, and industry laws, regulations, and directives that may affect this E-mail Archiving and Retention Policy.

2.3 Phoenix IT's responsibilities

Phoenix IT Department is responsible for implementing and supporting an appropriate data archiving solution and supporting software.

Any and all archived data will be tagged with metadata in order to make data headers, content, attachments, and text fully searchable. In addition, Phoenix IT Department will deploy and maintain software applications that support the archiving and search ability of stored data.

2.4 Data classification

The following is a list of types and categories which should be used to classify data. Any data which would not fall under any of these categories must be assessed by Phoenix Management and Phoenix IT Department to determine its retention guidelines :

2.4.1 Administrative Correspondence

- Phoenix Administrative Correspondence includes clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with information sent to or from the Phoenix Management Staff shall also be treated as Administrative Correspondence.

2.4.2 Fiscal Correspondence

- Phoenix Fiscal Correspondence is all information related to revenue and expense for Phoenix. It especially includes any financial reporting related correspondence.

2.4.3 General Correspondence

- Phoenix General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for data retention of General Correspondence.

2.4.4 Ephemeral Correspondence

- Phoenix Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

2.4.5 Customer Sensitive or Confidential Information

- See Data Classification Policy for description.
- Data should be destroyed upon completion of related projects as agreed to with customers.
- Data that changes in classification to public based on its age, should be destroyed according to need for computing, backup, and storage resources.

2.5 Record Retention Schedule

The Phoenix Management is responsible for creating and maintaining a list (called "***Record Retention Schedule***") of all data categories and types created and maintained by Phoenix that qualify as business records or messages that must be archived under the law.

The Phoenix IT Department will assist Phoenix Management in maintaining this schedule.

For each data type, a mandatory retention schedule and method of disposal must be stipulated, in addition to storage locations.

2.6 Policy Suspension

In some instances, this E-Mail Archiving and Retention Policy may be temporarily suspended, specifically if an investigation, litigation, or audit is anticipated. In some instances, this policy's disposal schedule may conflict with the need to produce data relevant to the aforementioned legal or regulatory procedures. If this is the case, then the need to comply fully with the law and/or regulation will override this policy, causing this policy to be temporarily suspended until the matter in question is satisfactorily resolved. Suspension of this policy will take the form of no data being disposed of whatsoever for a period of time, until lifted.

2.7 Policy Non-Compliance

It is in violation of this policy to dispose of any data types named in the Retention Schedule above.

PHOENIX PERSONNEL SECURITY POLICY

Table Of Contents

1 Purpose 3

2 Policy Statement 3

2.1 SECURITY IN JOB DEFINITIONS 3

2.1.1 Including Security In Job Responsibilities 3

2.1.2 Personnel Screening 3

2.1.3 Non Disclosure Agreements 3

2.1.4 Terms And Conditions Of Employment 3

2.2 USER TRAINING 4

2.2.1 Information Security Awareness And Training 4

2.3 RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS 4

2.3.1 Reporting Security Incidents, Weaknesses and Malfunctions 4

2.3.2 Learning From Incidents 4

1 Purpose

In accordance with industry 'best practices' and to comply with numerous compliance regulations, Phoenix has prepared various Information Security policies and procedures which are intended to protect the confidentiality, integrity and availability (CIA) of their critical client data and their computing resources. This document describes personal security policy at Phoenix in defining and administering these policy and procedures.

2 Policy Statement

Personnel at all levels are required to contribute to maintaining a high level of information security. As stated in the Corporate Security Policy, '*security is a business objective where staff members are to be active agents and is an integral part of everybody's job profile and objectives*."

This document lays out Phoenix's Information Security Policies relating to Phoenix's employees, and other users of Phoenix's information systems. It includes security in job definitions, user training, and responding to security incidents and malfunctions.

2.1 Security In Job Definitions

2.1.1 Including Security In Job Responsibilities

2.1.1.1 All job roles and responsibilities must be documented and should include general as well as specific responsibilities for implementing or maintaining security within Phoenix.

2.1.1.2 All employees of Phoenix must understand their job roles and responsibilities.

2.1.2 Personnel Screening

2.1.2.1 Periodic background checks should be performed on all personnel who work in sensitive or critical job roles.

2.1.2.2 All supervisory roles are responsible for the performance and conduct of the staff personnel reporting to them. Managers/supervisors are required to monitor performance and conduct of each of their staff. Information owners and business process owners must assess the impact on the security of the information resources to which the staff has access.

2.1.3 Non Disclosure Agreements

2.1.3.1 All users of Phoenix's information assets will be required to accept non-disclosure obligations. Users are required not to disclose company or customer information derived as a result of their access to Phoenix's information systems to unauthorized parties.

2.1.3.2 All users will be required to periodically re-affirm their non-disclosure obligations by signing non-disclosure and/or confidentiality agreements.

2.1.4 Terms And Conditions Of Employment

2.1.4.1 Phoenix's employment polices must contain reference to:

- The employee's legal and security related responsibilities,
- The extent and duration of the responsibilities

- An indication of management action in case the terms of employment are violated.

2.1.4.2 All employees of Phoenix must sign a statement indicating they read and accept the terms of the Acceptable use policy.

2.2 User Training

2.2.1 Information Security Awareness and Training

2.2.1.1 Each employee, with access to sensitive information, must be educated with regards to information security and security awareness. Additionally, those who are involved with technical security responsibilities are required to learn additional security skills that correspond to their specific job role.

2.2.1.2 Details of training and certificates (if any) issued during the training must be documented and maintained in each personnel's profile.

2.3 Responding To Security Incidents And Malfunctions

2.3.1 Reporting Security Incidents, Weaknesses and Malfunctions

2.3.1.1 All Phoenix employees and business partners are responsible for reporting of any security breaches, security weaknesses, or software malfunctioning, to the Phoenix IT department, or the legal department, as quickly as possible using the Incident Report Form, or e-mail, or and direct contact.

2.3.2 Learning From Incidents

2.3.2.1 Phoenix requires that processes be developed to analyze security incidents and identify proactive measures to be undertaken to avoid similar incidents in future.

Phoenix Settlement Administration
Office Risk Assessment

Management Unit:	Phoenix Settlement Administration	**Location:** (Site/ Building/ Room)	
Assessment Date:		**Review Date:**	
Assessors Name:		**Job Title:**	
Task: Risk assessment for the activities associated with work in an office environment.			

What are the hazards? (See list of sample hazards)	Who might be harmed? (e.g. Staff, students, visitors)	What are the risks	Are the following control measures in place to eliminate or reduce the risks?	Yes/ No	Corrective actions required	Risk Evaluation			Risk Rating
						Consequence (1 – 3)	Likelihood (1 – 3)	Overall risk (C x L)	Low, Medium or High
Slips, trips and falls		Could suffer injury e.g. sprains and fractures if they trip and fall as a result of: • Obstructions, trailing cables, spillages, worn or raised floor coverings etc on walkways. • Poor office layout and storage arrangements resulting in insufficient circulation space.	1. Work areas should be kept clear of obstructions. 2. Any spillages should be cleaned up immediately. 3. All areas should be well lit, especially stairs. 4. Any hazards such as torn carpets, trailing cables, defects to floor coverings, faulty lighting etc. should be reported immediately to the line manager or local person responsible for safety.						
Manual Handling		Could suffer from back pain and work related upper body disorder (WRULD) due to: • Using incorrect handling techniques when handling office items (deliveries, boxes, filing etc).	1. A risk assessment must be completed for lifting heavy and bulky loads that present a risk of injury e.g. stretching, stooping, twisting). 2. A trolley should be used to transport boxes of paper or other heavy items. 3. Using low shelves for storing heavy items and only using						

What are the hazards? (See list of sample hazards)	Who might be harmed? (e.g. Staff, students, visitors)	What are the risks	Are the following control measures in place to eliminate or reduce the risks?	Yes/ No	Corrective actions required	Risk Evaluation			Risk Rating
						Consequence (1 – 3)	Likelihood (1 – 3)	Overall risk (C x L)	Low, Medium or High
		• Poor workstation layout and insufficient working space resulting in poor posture. • Individuals with health conditions, previous back injuries etc affecting ability to safely handle items • New and expectant mothers may be more susceptible to injury.	high shelves for light items only. 4. Training in lifting techniques should be provided for anyone who undertakes lifting of heavy loads.						
Computer workstation use		WRULD could develop as a result of • Inappropriate layout or lack of awareness resulting in poor posture being adopted when using Display Screen Equipment (DSE) • Working for prolonged periods without change of posture or sufficient break.	1. Where desktops, laptops and notebooks are used as a significant part of day-to-day work, a Computer Equipment assessment must be carried out. 2. Work should be planned to include regular breaks from the computer. 3. HSE leaflet “Are you keying safely” may be issued to DSE users.						
Data loss		Removed data in a result of • Accidental deletion • Software and/or hardware failure	1. Proper access rights are set in place to prevent deletion of critical data. 2. Regular local and offsite backups are in place and monitored.						

What are the hazards? (See list of sample hazards)	Who might be harmed? (e.g. Staff, students, visitors)	What are the risks	Are the following control measures in place to eliminate or reduce the risks?	Yes/ No	Corrective actions required	Risk Evaluation			Risk Rating
						Consequence (1 – 3)	Likelihood (1 – 3)	Overall risk (C x L)	Low, Medium or High
			3. Proper training of the staffs on using computers and how data are handled.						
Electrical safety		Could suffer electrical shock or burns if using • Damaged portable electrical appliances, their cables, plugs e.g. lamps, fans, photocopier, extension leads, PC etc.	1. All portable electrical equipment must be tested for electrical safety at correct intervals and labelled with the date of the test. 2. Electrical cables and plugs should be regularly visually inspected by the user for damage. 3. Any defective equipment should be reported immediately to the responsible person e.g. line manager or local safety coordinator, then suitably labelled and taken out of use until the repair has been carried out. 4. Electrical equipment must always be operated in accordance with manufacturers' instructions.						
Fire		Could suffer from smoke inhalation or burns if trapped in office. • Combustible materials coming into contact with or in close proximity to heat sources.	1. The storage of empty cardboard boxes should be kept to an absolute minimum. 2. Equipment should be switched off when not in use for long periods. 3. All portable electrical equipment must be tested for						

What are the hazards? (See list of sample hazards)	Who might be harmed? (e.g. Staff, students, visitors)	What are the risks	Are the following control measures in place to eliminate or reduce the risks?	Yes/ No	Corrective actions required	Risk Evaluation			Risk Rating
						Consequence (1 – 3)	Likelihood (1 – 3)	Overall risk (C x L)	Low, Medium or High
		• Portable heaters in unsafe condition and/or inappropriately located. • Over accumulation of rubbish. • Over loading of electrical sockets. • Inappropriate action in the event of discovering a fire or hearing the fire alarm.	electrical safety at appropriate intervals. 4. The fire alarm system is installed, maintained and tested. 5. Fire risk assessments for each building should be carried out periodically. 6. Everyone must be acquainted with the Emergency evacuation procedure for their area. 7. Area Fire Officers and depute must be appointed to cover offices and general areas.						
Lone working and Out of Hours work (LOOH)		Staff unable to promptly summon emergency assistance in the event of serious injury, sudden illness or personal threat.	1. LOOH work should be minimised or avoided where feasible. 2. If unavoidable, conduct a generic LOOH Risk Assessment 3. Specific LOOH Risk Assessment may be required in circumstances where any potential risks are increased (e.g. expectant mothers, persons with mobility issues or medical conditions).						
Falling from height		• Falling when retrieving items stored at height • Dropping items onto others when stored at height	1. Chairs or desks must not be used for reaching heights; step stools should be used instead. 2. If a stepladder is used, staff/students should read an appropriate risk assessment						

What are the hazards? (See list of sample hazards)	Who might be harmed? (e.g. Staff, students, visitors)	What are the risks	Are the following control measures in place to eliminate or reduce the risks?	Yes/ No	Corrective actions required	Risk Evaluation			Risk Rating
						Consequence (1 – 3)	Likelihood (1 – 3)	Overall risk (C x L)	Low, Medium or High
			and be shown how to use it safely. 3. To prevent injuries heavy items must not be stored on upper shelves. They should be stored at waist height.						
Working environment		• May feel too hot/cold or suffer other general discomfort • Contact with furniture if insufficient space to move around. • May suffer eyestrain if lighting is insufficient or of the wrong type	1. Is the temperature of the office normally kept within a comfortable range? 2. Is the office adequately ventilated? 3. Is the space provided is sufficient to enable free movement around the office, and for carrying out general tasks? 4. Are the lighting levels adequate for the tasks undertaken? 5. Are window blinds fitted where necessary to adjust lighting levels? 6. Are desk lamps provided if additional task lighting is required?						
Inadequate hygiene and welfare facilities		General discomfort or stress.	1. Are toilets supplied with hot/cold water, soap and towels, and deficiencies reported to the cleaning staff? 2. Is an area available for refreshment with drinking water available? 3. Is the 'No smoking' policy implemented?						

What are the hazards? (See list of sample hazards)	Who might be harmed? (e.g. Staff, students, visitors)	What are the risks	Are the following control measures in place to eliminate or reduce the risks?	Yes/ No	Corrective actions required	Risk Evaluation			Risk Rating
						Consequence (1 – 3)	Likelihood (1 – 3)	Overall risk (C x L)	Low, Medium or High
Chemical risks		Generally the risk will be very low within an office environment.	If any hazardous substances e.g. solvents or solvent-based glues are used within the office area then a COSHH risk assessment must be completed and a safe system of work issued to the users.						
Filling Cabinets		• Could topple over if loading is unbalanced. • Cabinet drawers that have been left open could be a trip hazard	1. Filing cabinets should be loaded from the bottom up to maintain stability. 2. Where filing cabinets are of the type that allows more than one drawer to be opened at a time, they must be labelled with a warning of a tipping risk. 3. Drawers should be closed immediately after use.						
Office equipment		Coming into contact with moving, cutting or other dangerous parts, clothing, long hair etc becoming entangled. e.g. shredders, guillotines	1. Equipment used in accordance with manufacturer's instructions 2. Those using the equipment have been made aware of how to use it safely e.g. verbal instruction, signage etc. 3. Equipment periodically checked for safe condition and taken out of use if any damage found.						

What are the hazards? (See list of sample hazards)	Who might be harmed? (e.g. Staff, students, visitors)	What are the risks	Are the following control measures in place to eliminate or reduce the risks?	Yes/ No	Corrective actions required	Risk Evaluation			Risk Rating
						Consequence (1 – 3)	Likelihood (1 – 3)	Overall risk (C x L)	Low, Medium or High
			4. Loose clothing (e.g. ties) and long hair kept away from any moving parts.						
Any other hazards identified?									

1. EXAMPLE HAZARDS THAT MAY BE APPLICABLE TO THE JOB or WORK ACTIVITY			
Working at Height	Noise	Hand tools	Vibration
Falling objects	Extreme Heat / cold	Confined spaces	Repetitive hand/ arm movement
Slippery/ uneven/ worn floors	Radiation	Poor housekeeping / cleaning	Machine operation
Obstructions/ projections	Lighting	Vehicle movement	Electro Magnet
Manual handling	Compressed air	Fire / explosion	Pressurised systems
Mechanical Lifting	Substances / materials	Electricity	**Other (*specify on assessment)***

2. RISK MATRIX		Potential consequence of harm		
		1 – Minor Injury (e.g. hazard can cause illness, injury or equipment damage but the results would not be expected to be serious)	**2 – Significant Injury** (e.g. hazard can result in serious injury and/or illness, over 3 day absence)	**3 – Major Injury** (e.g. hazard capable of causing death or serious and life threatening injuries)
Likelihood of harm	**1 – Unlikely** (injury rare, though possible)	**1 – Low**	**2 – Low**	**3 – Medium**
	2 – Possible (injury could occur occasionally)	**2 – Low**	**4 – Medium**	**6 – High**
	3 – Probable (injury likely to occur, can be expected)	**3 – Medium**	**6 – High**	**9 – Extreme**

3. RISK EVALUATION

This is calculated by multiplying the likelihood against the consequence e.g. taking a likelihood of 1, which is classified as Unlikely and multiplying this against a Potential Consequence of 2, which is classified as Significant Injury, would give you and overall Risk Rating of 2, which would result in an overall evaluation as a low risk.

1 to 2 = **Low risk**

Low risks are largely acceptable, monitor periodically to determine situation changes which may affect the risk, or after significant changes

3 to 4 = **Medium risk**

Medium risks at the upper end of this band should only be tolerated for the short-term and then only whilst further control measures to mitigate the risk are being planned and introduced, within a defined time period. Risks on the lower end should be reduced if practicable.

6 = High risk

High risks activities should cease immediately until further control measures to mitigate the risk are introduced. The continued effectiveness of control measures must be monitored periodically.

9 = Extreme Risk

Work should not be started or continued until the risk has been mitigated. Immediate action is required to reduce exposure. A detailed mitigation plan must be developed, implemented and monitored by senior management to reduce the risk before work is allowed to commence.

PHOENIX'S SERVICE PROVIDER RISK ASSESSMENT

1. **Understand the depth of the relationships your firm has established.**

   Understanding of who your outsourced providers are, what services/functions they provide and what level of access they have to your firm's data/systems.

   Here is a quick list of possible third parties:

   - IT infrastructure/cloud provider/managed security service
   - Legal consultant(s)
   - Auditing/tax firm/accounting
   - Outsource Printing
   - Outside contractors: Equipment Repair

2. **Calculate potential risks and vulnerabilities.**

   Assessing provider access to data, systems, financials or other proprietary data. Completing a provider risk assessment for each third-party engagement, provide insight into the level of access each provider has and hence, any potential vulnerabilities that may arise.

3. **Conduct thorough due diligence before the relationship commences.**

   Conduct initial vetting, sending requests for proposals, assessment of documentation and gathering as much information as possible.

4. **Continue conducting proper due diligence throughout the course of the relationship.**

   Continuously evaluated and monitored to ensure both parties are achieving their end goals and meeting expectations. General monitoring of service provider practices and performance. Engaging with compliance consultants and auditing firms to conduct independent service provider evaluations and assessments.

5. **Employ contingency plans for terminating vendor contracts.**

   Review for any contractual loopholes and operational practices that may affect migration plans or your firm's security standing.

Information Classification and Access Control Policy

Dated: 4/27/2022
Reviewed: Annually
Domains: Asset Classification and Control
Communications and Operations Management
Physical and Environmental Security
Information Security Incident Management

POLICY STATEMENT

1. Millennium Systems (MS) Responsibility—All MS employees who come into contact with sensitive *Phoenix Settlement Administration* internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily *Phoenix Settlement Administration* business activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, MS employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for MS for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

2. Addresses Major Risks - The MS data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect *Phoenix Settlement Administration* information from unauthorized disclosure, use, modification, and deletion.

3. Applicable Information - This data classification policy is applicable to all electronic information for which MS is the custodian.

PROCEDURES

1. Access Control

1.1 Need to Know—Each of the policy requirements set forth in this document are based on the concept of need to know. If an MS employee is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information.

1.2 System Access Controls—The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to *Phoenix Settlement Administration* systems and their resources. Remote access shall be controlled through identification and authentication mechanisms.

1.3 Access Granting Decisions—Access to *Phoenix Settlement Administration* sensitive information must be provided only after the written authorization of the Data Owner has been obtained. Access requests will be presented to the data owner using the Access Request template. Custodians of the involved information must refer all requests for access to the relevant Owners or their delegates.

Special needs for other access privileges will be dealt with on a request-by-request basis. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by the

relevant Data Owner in accordance with a system review schedule approved by the VP, Director of Information Services and the AVP, Director of Risk Management.

2. Information Classification

2.1 Owners and Production Information—All electronic information managed by MS must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners should be at the VP level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the *Phoenix Settlement Administration* management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

2.2 RESTRICTED—This classification applies to the most sensitive business information that is intended for use strictly within *Phoenix Settlement Administration*. Its unauthorized disclosure could seriously and adversely impact *Phoenix Settlement Administration*, its customers, its business partners, and its suppliers.

2.3 CONFIDENTIAL—This classification applies to less-sensitive business information that is intended for use within *Phoenix Settlement Administration*. Its unauthorized disclosure could adversely impact *Phoenix Settlement Administration* or its customers, suppliers, business partners, or employees.

2.4 PUBLIC—This classification applies to information that has been approved by *Phoenix Settlement Administration* management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

2.5 Owners and Access Decisions—Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. MS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

3. Object Reuse and Disposal

Storage media containing sensitive (i.e. restricted or confidential) information shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the Director of MS Security.

4. Physical Security

4.1 Data Center Access—Access to the data center must be physically restricted in a reasonable and appropriate manner.

4.2 Facility Access–All network equipment (routers, switches, etc.) and servers located in the corporate office and in all facilities must be secured when no *Phoenix Settlement Administration* personnel, or authorized contractors, are present. Physically secured is defined as locked in a location that denies access to unauthorized personnel.

4.3 Removal of Access- Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access *Phoenix Settlement Administration* systems.

4.4 User Verification- A verification of the user's identity must be performed by the Operations Director before granting a new password.

4.5 Annual Review- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

4.5.1. An active account assigned to employees that no longer work for the Institution.

4.5.2. An active account with access rights for which the user's role and responsibilities do not require access.

6.8.3. System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.

5. Special Considerations for Restricted Information

If Restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must conform to data access control safeguards approved by MS and Corporate senior management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

5.1 Data Encryption Software—*Phoenix Settlement Administration* employees and vendors must not install encryption software to encrypt files or folders without the express written consent of MS Security.

6. Information Transfer

6.1 Transmission Over Networks—If *Phoenix Settlement Administration* Restricted data is to be transmitted over any external communication network, it must be sent only in encrypted form. Such networks include electronic mail systems, the Internet, etc. All such transmissions must use a virtual public network or similar software as approved by the Information Security Team.

6.2 Transfer to Another Computer—Before any Restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

6.3 Accuracy of data- responsibility belong solely to the transferring entity.

7. Software Security

7.1 Secure Storage of object and source code—Object and source code for system software shall be securely stored when not in use by the developer. Developers must not have access to modify program files that actually run in production. Changes made by developers must be implemented into production by Technical Operations. Unless access is routed through an application interface, no developer shall have more than read access to production data. Further, any changes to production applications must follow the change management process.

7.2 Testing—Developers must at least perform unit testing. Final testing must be performed by the Quality Assurance team or the target user population.

7.3 Backups—Sensitive data shall be backed up regularly, and the backup media shall be stored in a secure environment.

8. Key Management

8.1 Protection of Keys—Public and private keys shall be protected against unauthorized modification and substitution.

8.2 Procedures—Procedures shall be in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

8.3 Safeguarding of Keys—Procedures shall be in place to safeguard all cryptographic material, including certificates. MS Security must be given copies of keys for safekeeping.

9. Phoenix Settlement Administration Employees and Vendors—All above policies apply to all employees of both PSA and any third-party service providers who can access the data provided to PSA.

Phoenix Settlement Administrator
Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Phoenix Settlement Administrator's (PSA) entire network. As such, all PSA employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any PSA facility, has access to the PSA network, or stores any non-public PSA information.

4.0 Policy

4.1 General

- All system-level passwords must be changed every 90 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every 90 days
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at PSA. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than sixteen characters
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.

- Computer terms and names, commands, sites, companies, hardware, software.
- The words "PSA", "Class Action" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9 ,!@#$%^&*()_+|- =\`{}[]:";'<>?,./)
- Are at least sixteen alphanumeric characters long.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

B. Password Protection Standards

Do not use the same password for PSA accounts as for other non-PSA access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various PSA access needs. Do not share PSA passwords with anyone, including administrative assistants or secretaries.

All passwords are to be treated as sensitive, confidential PSA information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to your supervisor
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the management.

Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, Instant Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system without encryption.

Change passwords at least once every 90 days.

If an account or password is suspected to have been compromised, report the incident to the management and change all passwords.

C. Remote Access

Access to the PSA Networks via remote access is controlled using Virtual Private Networking (VPN). VPN can be setup by notifying the management and the Technology Group (Millennium Systems)

D. Passwords at Account Creation

When a request for a username is requested, the management will determine the type and privileges required. The password will be set to be pre-expired so the user will be required to change their password when they first successfully logon to the system. The lifetime of the password will be set according to the guidelines set in section 4.1 of this document.

E. Forgotten Passwords

Users will occasionally forget their password. A characteristic of password files is that passwords cannot be looked up. If a user forgets their password, the password can be changed by Millennium Systems.

5.0 Enforcement

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

Certificate of Data Destruction

Phoenix Settlement Administration.

The requested data is destroyed using the one or more of the following method(s):

Data Destruction Procedure:

- ❑ 1-Pass partial wipe: The data was removed from the server and software was used to overwrite empty section of the storage and indexing locations with zeros (0x00) once and then verified
- ❑ 1-Pass full wipe: Software was used to overwrite all addressable storage hardware and indexing locations with zeros (0x00) once and then verified
- ❑ 3-Pass full wipe: Software was used to overwrite all addressable storage hardware and indexing locaitons on the drive three times with zeros (0x00), complement (0xFF) and random characters and then verified.
- ❑ Shred: Shredded according to the National Institute of Standards and Technology's (NIST) Special Publication 800-88 Guidelines for Media Sanitization.
- ❑ Crushed: Hard drives were placed inside a specialized machine and a conical punch inside the unit delivered 12,000 pounds of hydraulic force to the drive, causing catastrophic trauma to the hard drive's chassis, destroying its internal platter, and then shredded according to the National Institute of Standards and Technology's (NIST) Special Publication 800-88 Guidelines for Media Sanitization.

Company Name:

Date:

SECURITY AWARENESS TRAINING PROGRAM

Table of Contents

1. **General**
    - A. **Introduction to Computer Security**
    - B. **Beware of Scams**
    - C. **Protect Information when using the Internet and email**
    - D. **Protect Passwords**
    - E. **Mobile Devices and Wireless**

2. **Working with Different Types of Data**
    - A. **Categories of Data**
    - B. **More About Restricted Data**
    - C. **Protecting Restricted Data**
    - D. **Report a Security Incident**

3. **Other Essential Security Measures**
    - A. **Install Operating System and Software Updates**
    - B. **Don't Download Unknown or Unsolicited Programs or Files**
    - C. **Lock your computer screen**
    - D. **Physical Security**
    - E. **Protect Your Passwords**
    - F. **Travel Securely**
    - G. **Back Up Important Files**

EXHIBIT E

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 2/5/2026

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Inszone Insurance Services, LLC
2721 Citrus Road, Suite A
Rancho Cordova, CA 95742

License#: 0F82764

CONTACT NAME: Certificate Team
PHONE (A/C, No, Ext): 877-308-9663 **FAX (A/C, No):** 916-400-2625
E-MAIL ADDRESS: certs@inszoneins.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Hartford Underwriters Insurance Company	30104
INSURER B : Travelers Excess and Surplus Lines Company	29696
INSURER C : Hartford Casualty Insurance Company	29424
INSURER D : Gemini Insurance Company	10833
INSURER E : At-Bay Specialty Insurance Company	19607
INSURER F : Scottsdale Insurance Company	41297

INSURED
Phoenix Settlement Administrators
1411 North Batavia Street
Orange, CA 92867-3526

PHOESET-02

COVERAGES **CERTIFICATE NUMBER:** 88541127 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X **COMMERCIAL GENERAL LIABILITY** CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: X POLICY PRO-JECT LOC OTHER:			57SBABD5BWA	3/4/2025	3/4/2026	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$ 1,000,000 $ 1,000,000 $ 10,000 $ 1,000,000 $ 2,000,000 $ 2,000,000
	AUTOMOBILE LIABILITY ANY AUTO OWNED AUTOS ONLY SCHEDULED AUTOS HIRED AUTOS ONLY NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$ $ $ $
B	**UMBRELLA LIAB** X OCCUR X **EXCESS LIAB** CLAIMS-MADE DED RETENTION $			CXS-108157224-01	1/19/2026	1/19/2027	EACH OCCURRENCE AGGREGATE	$ 2,000,000 $ 2,000,000
C	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** Y / N ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		57WECAB4EGD	5/1/2025	5/1/2026	X PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ 1,000,000 $ 1,000,000 $ 1,000,000
D E F	Professional Liability Cyber Liability Employment Practices Liability			VNPL020810 AB-6755733-03 EKS3585841	1/19/2026 1/19/2026 8/12/2025	1/19/2027 1/19/2027 8/12/2026	Aggregate/Each Claim Aggregate Aggregate	$2,000,000 $3,000,000 $2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Verification Of Insurance

CERTIFICATE HOLDER

Verification Of Insurance

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

© 1988-2015 ACORD CORPORATION. All rights reserved.

EXHIBIT F

PHOENIX

CLASS ACTION ADMINISTRATION SOLUTIONS

CASE ASSUMPTIONS	
Class Members	205
Opt Out Rate	1%
Opt Outs Received	2
Total Class Claimants	203
Subtotal Admin Only	**$7,950.00**
Not-to-Exceed Total	**$7,950.00**

For 205 Members

Pricing Good for Scope of Estimate Only

June 3, 2026

Case: Hernandez, et al. v. Gold Point Transportation Opt-Out Administration wTranslation

Phoenix Contact: Jodey Lawrence
Contact Number: 949.566.1455
Email: Jodey@phoenixclassaction.com

Requesting Attorney: Scott Lidman
Firm: LIDMAN LAW, APC
Contact Number: (424) 322-4774
Email: Slidman@lidmanlaw.com

Assumptions and Estimate are based on information provided by counsel. If class size changes, PHX will need to adjust this Estimate accordingly. Estimate is based on 205 Class Members. Class data **Must** be sent in Microsoft Excel or uploaded in the same format. Class Data Must be sent in one spreadsheet, with no additional programming needed. A rate of $150 per hour will be charged for any additional analysis or programming. Pricing good for 90 days.

Case & Database Setup / Toll Free Setup & Call Center / NCOA (USPS)			
Administrative Tasks:	**Rate**	**Hours/Units**	**Line Item Estimate**
Programming Manager	$125.00	2	$250.00
Programming Database & Setup	$125.00	2	$250.00
Toll Free Setup*	$144.33	1	$144.33
Call Center & Long Distance	$2.00	16	$32.00
NCOA (USPS)	$145.00	2	$290.00
		Total	**$966.33**

* Up to 120 days after disbursement

Data Merger & Scrub / Notice Packet, Opt-Out Form & Postage / Translation / Reporting			
Project Action	**Rate**	**Hours/Units**	**Line Item Estimate**
Notice Packet Formatting	$125.00	3	$375.00
Data Merge & Duplication Scrub	$0.35	205	$71.75
Notice Packet & Opt-Out Form	$1.25	205	$256.25
Estimated Postage (up to 2 oz.)*	$0.79	205	$161.95
Static Website	$250.00	1	$250.00
Language Translation	$1,000.00	1	$1,000.00
		Total	**$2,114.95**

* Prices good for 90 days. Subject to change with the USPS Rate or change in Notice pages or Translation, if any.

PHOENIX

CLASS ACTION ADMINISTRATION SOLUTIONS

Skip Tracing & Remailing Notice Packets / Tracking & Programming Undeliverables			
Project Action:	**Rate**	**Hours/Units**	**Line Item Estimate**
Case Associate	$55.00	2	$110.00
Skip Tracing Undeliverables	$2.00	14	$28.70
Remail Notice Packets	$1.75	14	$25.11
Estimated Postage	$0.79	14	$11.34
Programming Undeliverables	$50.00	2	$100.00
		Total	**$275.15**

Database Programming / Processing Opt-Outs, Deficiencies or Disputes			
Project Action:	**Rate**	**Hours/Units**	**Line Item Estimate**
Programming Claims Database	$135.00	1	$135.00
Non Opt-Out Processing	$200.00	1	$200.00
Case Associate	$55.00	2	$110.00
Opt-Outs/Deficiency/Dispute Letters	$10.00	3	$30.00
Case Manager	$85.00	2	$170.00
		Total	**$645.00**

Calculation & Disbursement Programming/ Create & Manage QSF/ Mail Checks			
Project Action:	**Rate**	**Hours/Units**	**Line Item Estimate**
Programming Calculations	$125.00	2	$250.00
Disbursement Review	$125.00	2	$250.00
Programming Manager	$95.00	2	$190.00
QSF Bank Account & EIN	$125.00	2	$250.00
Check Run Setup & Printing	$125.00	2	$250.00
Mail Class Checks *	$1.25	205	$256.25
Estimated Postage	$0.79	205	$161.95
		Total	**$1,608.20**

* Checks are printed on 8.5 x 11 in. sheets with W2/1099 Tax Filing

PHOENIX

CLASS ACTION ADMINISTRATION SOLUTIONS

Tax Reporting & Reconciliation / Re-Issuance of Checks / Conclusion Reports and Declarations			
Project Action:	**Rate**	**Hours/Units**	**Line Item Estimate**
Case Supervisor	$125.00	3	$375.00
Remail Undeliverable Checks (Postage Included)	$1.50	10	$15.38
Case Associate	$55.00	2	$110.00
Reconcile Uncashed Checks	$85.00	2	$170.00
Conclusion Reports	$125.00	2	$250.00
Case Manager Conclusion	$85.00	2	$170.00
Final Reporting & Declarations	$125.00	2	$250.00
IRS & QSF Annual Tax Reporting * (1 State Tax Reporting Included)	$1,000.00	1	$1,000.00
		Total	**$2,340.38**

* All applicable California State & Federal taxes, which include SUI, ETT, and SDI, and FUTA filings. Additional taxes are Defendant's responsibilty.

Estimate Total: $7,950.00

PHOENIX

CLASS ACTION ADMINISTRATION SOLUTIONS

TERMS AND CONDITIONS

Provisions: The case estimate is in good faith and does not cover any applicable taxes and fees. The estimate does not make any provision for any services or class size not delineated in the request for proposal or stipulations. Proposal rates and amounts are subject to change upon further review, with Counsel/Client, of the Settlement Agreement. Only pre-approved changes will be charged when applicable. No modifications may be made to this estimate without the approval of PSA (Phoenix Settlement Administrators). All notifications are mailed in English language only unless otherwise specified. Additional costs will apply if translation into other language(s) is required. Rates to prepare and file taxes are for Federal and California State taxes only. Additional charges will apply if multiple state tax filing(s) is required. **Pricing is good for ninety (90) days.**

Data Conversion and Mailing: The proposal assumes that data provided will be in ready-to-use condition and that all data is provided in a single, comprehensive Excel spreadsheet. PSA cannot be liable for any errors or omissions arising due to additional work required for analyzing and processing the original database. A minimum of two (2) business days is required for processing prior to the anticipated mailing date with an additional two (2) business days for a National Change of Address (NCOA) update. Additional time may be required depending on the class size, necessary translation of the documents, or other factors. PSA will keep counsel apprised of the estimated mailing date.

Claims: PSA's general policy is to not accept claims via facsimile. However, in the event that facsimile filing of claims must be accepted, PSA will not be held responsible for any issues and/or errors arising out of said filing. Furthermore, PSA will require disclaimer language regarding facsimile transmissions. PSA will not be responsible for any acts or omissions caused by the USPS. PSA shall not make payments to any claimants without verified, valid Social Security Numbers. All responses and class member information are held in strict confidentiality. Additional class members are $10.00 per opt-out.

Payment Terms: All postage charges and 50% of the final administration charges are due at the commencement of the case and will be billed immediately upon receipt of the data and/or notice documents. PSA bills are due upon receipt unless otherwise negotiated and agreed to with PSA by Counsel/Client. In the event the settlement terms provide that PSA is to be paid out of the settlement fund, PSA will request that Counsel/Client endeavor to make alternate payment arrangements for PSA charges that are due at the onset of the case. The entire remaining balance is due and payable at the time the settlement account is funded by Defendant, or no later than the time of disbursement. Amounts not paid within thirty (30) days are subject to a service charge of 1.5% per month or the highest rate permitted by law.

Tax Reporting Requirements

PSA will file the necessary tax returns under the EIN of the QSF, including federal and state returns. Payroll tax returns will be filed if necessary. Under the California Employment Development Department, all taxes are to be reported under the EIN of the QSF with the exception of the following taxes: Unemployment Insurance (UI) and Employment Training Tax (ETT), employer-side taxes, and State Disability Insurance (SDI), an employee-side tax. These are reported under Defendant's EIN. Therefore, to comply with the EDD payroll tax filing requirements we will need the following information:

1. Defendant's California State ID and Federal EIN.

2. Defendant's current State Unemployment Insurance (UI) rate and Employment Training Tax (ETT) rate. This information can be found in the current year DE 2088, Notice of Contribution Rates, issued by the EDD.

3. Termination dates of the class members, or identification of current employee class members, so we can account for the periods that the wages relate to for each class member.

4. An executed Power of Attorney (Form DE 48) from Defendant. This form is needed so that we may report the UI, SDI, and ETT taxes under Defendant's EIN on their behalf. If this form is not provided we will work with the EDD auditors to transfer the tax payments to Defendant's EIN.

5. Defendant is responsible for reporting the SDI portion of the settlement payments on the class member's W-2. PSA will file these forms on Defendant's behalf for an additional fee and will issue an additional W-2 for each class member under Defendant's EIN, as SDI is reported under Defendant's EIN rather than the EIN of the QSF. The Power of Attorney (Form DE 48) will be needed in order for PSA to report SDI payments.