Introduction

This Incident Response Plan exists to ensure that we consistently handle information security events in an effective and efficient manner. By doing so we can minimise negative consequences to the organisation, our staff, customers and other people we hold data on. This response plan is meant to address privacy/security incidents involving any and all Tinkerbell Aerial Freight data, including Tinkerbell data under the control or responsibility of a Business Associate or other third party.

Coordinating our response

We primarily use Slack to coordinate our response to cyber security events. We also use a conference call for update calls. If an issue is classified as a S1 or S2 we will create a channel in Slack specifically for that issue and include the relevant individuals and assign roles at that time.

Slack:	https://tinkerbellaf.slack.com/incident-response
Conference call:	+1 123 456 7890, meeting ID: 123456#
One-click join:	+1 123 456 7890,,,123456#

Alternative communication methods may be used or required if, for example, email or Slack accounts are believed to have been compromised and are unavailable, or their use would tip-off an adversary.

Phone numbers, email and other details on individuals and our key suppliers can be found in key contacts.

Detect and Respond

When a privacy incident is reported or detected:

- Log the incident
    - Manager's name
    - Notification Source
    - Notification Time
    - Systems Affected
    - Data Exposed
    - Other Details
- Form a working hypothesis for the incident
- Assign an incident severity
    - S1-S4, as defined by the severity matrix
- Assign an incident category
    - As defined by the categorization appendix

- Escalate or notify (as required)
    - No escalation needed for S4 and S3
- Mobilize Privacy IR Team based on type and severity of the incident
- Consider the need for Law Enforcement involvement
- Consider the need to notify data protection officer and regulator
- Consider the need for third-party support
- Consider need for Legal involvement
- Consider the need to notify any customer(s)

Contain

Data and logs should be sourced from data sources relevant to the investigation. Observation may involve detailed technical analysis to take large volumes of data (obtained from raw log files, or captured disk images) and conduct forensics to pull out important data points. If applicable, staff members closest to the incident will determine the extent of the incident by identifying all information (and systems) affected, and take action to stop the exposure. This may include:

Containment Checklist

- Identify what data is required to support testing the hypothesis
- Record the working hypothesis in the incident log
- Confirm which assets and data sources are in scope
- Gather direct observations (or request from supplier)
- Collate outside data (e.g. OSINT)
- Securing or disconnecting affected systems
- Securing affected records or documentation
- Halting affected business processes
- Pausing any processes that may rely on exposed information or that may have given rise to the incident (as necessary to prevent further use/exposure/etc)

This would most typically occur in instances of electronic system intrusion, exposed physical (e.g. medical) files or records or similar situations.

If the incident occurred at/by a third party, the Incident Response Team will determine if a legal contract and business associate agreement exist. The Compliance Officer and/or designee will work with the Legal Department and the department holding the contract/business associate agreement to review the contract terms and determine the next course of action.

Communicate

- Assess how an incident and the response to it may affect Tinkerbell's reputation and public image.
- Internal Communications

    - Determine the need to notify Administration at one, some or all Tinkerbell facilities
    - Determine the need to notify all current employees of the incident or employees of the affected facility or department only
    - Determine how employees will be notified (email, mail to home, mandatory staff meetings, etc.)
    - Determine who will communicate to the staff
    - Determine material content of the notification
- External Communications
    - Determine the need for external communications to covered entities, media (press conference or press release if Covered Entity is required to notify the media), etc.
    - Determine who will represent Tinkerbell publicly
    - Determine the material content of the Press Conference and/or Press Release
- Determine the need to post information regarding the incident to the company website

Notify

The Incident Response Team will determine what notifications are required and will make those notifications in a timely manner in accordance with federal law, state law, and organizational policy. Interaction between law enforcement and emergency services personnel should be coordinated by the Incident Response Commander. The Incident Response Commander will manage ongoing communication with authorities. It must be noted however that Law Enforcement's priorities are eventual prosecution of offenders and not necessarily returning the Company to a functional state. Ensure Legal is consulted and provides direction before and while communicating with Law Enforcement.

- Determine need to notify affected individuals according to applicable laws
- Determine all applicable regulators at state, federal and industry levels
- Determine if media notification is required
- Determine how all parties will be notified.
- Determine the content of the communications
- Deliver and document all required communications

Follow Up

After the initial response to the privacy incident, follow-up steps must be taken in order to prevent the event from recurring.

Investigation
Thorough investigation, and documentation of that investigation, is a critical component of incident response. Thorough investigation and documentation needs to be timely, accurate, and professional, and serves several purposes as listed below.

- Investigation goals
    - Show due diligence in complying with legal and regulatory requirements
    - Provide accurate and detailed report to management
    - Retain documentation that may be used in potential civil or criminal proceedings

Mitigation

Tinkerbell Aerial Freight has a legal and ethical obligation to mitigate (reduce) any harmful effects that result from privacy and security incidents. Though this is only legally required if we "have actual knowledge of harm," we will also take reasonable and appropriate steps to prevent harm from occurring either to individuals or to the Tinkerbell organization. Actual privacy/security incidents may result in negative outcomes for the affected parties several months or years later - we must acknowledge and be prepared to handle this risk appropriately.

- Mitigation Examples
    - In the event of exposed credit card information, we may need to provide "free" credit report monitoring and other "free" services that may be appropriate (such as credit counseling services or repeat medical testing) to affected individuals for a specified period of time.
    - Compliance, IT, and others may consult with Risk Management and Legal as necessary to understand the full scope of risks and potential damages and ways to mitigate.
    - Senior management may determine the need for any legal action to be taken on parties (internal or external) involved in the incident.
    - Responsible departments may determine the need for termination of a third party contract.
    - Tinkerbell] may contact third party insurers for services or resources related to any purchased policies (for instance, breach response services provided by a cyber-security policy).

Correction

Closely tied to mitigation, Correction should occur after any privacy or security incident in order to prevent future recurrence and to comply with organizational policy.

- Correction Examples
    - As appropriate, revise written policies and procedures that may be deficient.
    - Assess informal/unwritten processes and practices and make changes that correct or improve them.
    - Follow human resources policy and disciplinary action guidelines to determine need for disciplinary action on any Tinkerbell employee involved in the incident (Human Resources to be involved)
    - Determine the need for additional staff training.
    - Determine the need for increased security (physical or electronic) measures.

Review

Following the recovery phase, it is important to review the incident to fully understand the root causes of the events, where security monitoring and countermeasures may be improved, and other lessons learned. The output of post-incident reviews can also be used by the cyber security team to inform their cyber risk assessment.

Post-incident Reviews are conducted without blame or finger-pointing to encourage open and honest participation so that lessons can be learned and improvements identified. Failing to create the right open, safe environment may cause participants to withhold information crucial to preventing events from occurring again.

It is important to consider the people, process and technology aspects, and ‘what went well’ as well as ‘even better if,’ to continually improve the organisation’s capabilities. It is as important to recognise the good as it is to address any gaps.

The post-incident review will consider two lenses, including the:

- circumstances that led to the events themselves (“pre-event”)
- effectiveness and efficiency of the response activities (“post-event”)

Pre-event considerations (non-exhaustive!)

- Is this a common trend of similar events we are experiencing?
- What would have prevented the incident from occurring?
- How could we have detected the events sooner?
- Is this something considered by our cyber risk assessment?

Post-event considerations (non-exhaustive!)

- Was our response successful? (e.g. 1-10)
- What would have made our response more effective?
- How could we have made our response more efficient?
- Did we make a sound hypothesis?
- What was the key thing that led to us understanding the incident?
- Should we create, or update, a playbook for this scenario?
- Did anything hamper our response?
- Was any data or information difficult to obtain?
- Were the right people and tools available?
- Did we have any communication issues?

Review Checklist

- Identify stakeholders needed for post-incident review (inc. third-parties)
- Consider the need for independent facilitation
- Arrange a mutually convenient time for post-incident review
- Share incident report with attendees

- Discuss ‘what went well’ and ‘even better if’
- Do not ‘point fingers’ or assign blame to individuals
- Record the lessons learned and any further action points

Appendix

Severity matrix

When assessing the severity of an incident we consider the scale of the events, the type of systems and data involved, and the consequences. The severity matrix below helps to consistently apply severity ratings to incidents and includes some examples.

Severity	**Definition, escalation and typical cadence criteria...**
S1 (Very High)	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).
S2 (High)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
S3 (Moderate)	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
S4 (Low	individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).

Key contacts

Incident Management

Slack: https://tinkerbellaf.slack.com/incident-response
Conference call: +1 123 456 7890, meeting ID: 123456#
One-click join: +1 123 456 7890,,,123456#

Third-party support

We have an agreement with SomeTechCompany to provide subject matter expertise in the event of an incident.

They can be contacted at:

- +1 123 456 7890
- https://somemakebelievewebsite.co/#contact

Senior Management

Name	Contact	Deputy
Jane Director	jane@email.com 01234 567 890 07890 123 456 (24x7)	Bob Manager
Bob Manager	bob@email.com 01234 567 890 07890 123 456 (24x7)	Jo Leader
Jo Leader	jo@email.com 01234 567 890 07890 123 456 (24x7)	Bob Manager

Virtual IR team members

Name	Contact	Deputy

Other departmental leads

Name	Contact	Deputy
Legal		
Finance		
Human Resources		

Outsource IT provider

Name	Contact	Notes

Other key suppliers

Name	Contact	Notes

Incident categorization

a. Patient Privacy Complaints relating to
    i. Patient Privacy Rights
    ii. Communications
    iii. Inappropriate use, access or disclosure of health information
b. Employee-related Privacy Concerns relating to
    i. Inappropriate use, access or disclosure of health information
    ii. Inappropriate use, access or disclosure of confidential (non-health) information
    iii. Inappropriate modification, deletion or destruction of health information
c. Other Concerns relating to
    i. Loss or deletion of stored data; loss or theft of laptops, handheld devices, portable media storage containing confidential business or individually identifiable information
d. Theft or Loss of Tinkerbell Computer Equipment, including
    i. Desktop computers
    ii. Laptop computers
    iii. External hard drives
    iv. Compact disks/DVDs
    v. Blackberries/Tablets/PDAs
    vi. Thumb drives
    vii. Medical equipment that stores patient information
    viii. Any other device or storage media (whether issued by Tinkerbell or not) which may contain business records or personal information of any potential compromise of our patients, staff or affiliates
e. Computer/Network Intrusions, Data Losses, or other Compromises, including
    i. The unauthorized access, viewing, copying, forwarding, or removal of electronically stored data
    ii. Any other incidents that result/may result in unauthorized acquisition or release of any potential compromise of electronically stored business or patient information
f. Data Transmission Incidents, including
    i. Inadvertent email releases
    ii. Unsecured data transmission

Sources:

https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf
https://community.corporatecompliance.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=043e3710-465a-4e9c-9fce-6c0e15b715ce
https://frsecure.com/resource/incident-management-plan-template.pdf
https://cydea.tools/ir-plan/
https://iapp.org/media/pdf/resource_center/ENISA-breach-severity-methodology.pdf