Template Global Incident Response Policy [1]

Acme is fully committed to protecting the security and confidentiality of all of the personal information that is entrusted to us. As part of this commitment, Acme has documented and implemented this incident response policy to guide our internal handling of events and incidents that may impact "**Personal Information**," (sometimes called "Personal Data") which is any information that can be used identify, locate or contact an individual, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

A "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information. A Security Breach includes a "personal data breach" (as defined in the EU General Data Protection Regulation), a "breach of the security of a system" or similar term (as defined in any other applicable privacy) law as well as any other event that compromises the security, confidentiality or integrity of Personal Information.

Acme defines a **"Privacy Event"** as *any* occurrence that *could* compromise the privacy, confidentiality, security or integrity of Personal Information. Privacy Events include any deviation from Acme's privacy or security policies, loss of Personal Information as well as any unauthorized use or disclosure of Personal Information

Examples of Privacy Events:

- Lost or stolen device containing Personal Information
- Misdirected package, email or fax containing Personal Information
- Presence of malware on a computer or device containing Personal Information
- Transmission of Personal Information other than as permitted by company policy

Acme requires all employees and contractors to report Privacy Events as follows:

[add reporting process information]

We investigate all Privacy Events, to determine what happened, establish if any Personal Information was compromised, and (if so) evaluate the risk of harm that could result from the situation. *In many cases Privacy Events do not actually compromise any Personal Information. For example, Personal Information on a lost laptop may have been encrypted so that it could not be accessed or used by any unauthorized person.*

In some cases, Privacy Events do impact Personal Information. For example, a lost device may contain unencrypted information. Or an employee may have accidently transmitted a file containing Personal Information to the wrong recipient. If the recipient was able to view the Personal Information in the file,

[1] This template is provided for reference purposes only. Many countries have enacted laws with specific requirements for incident response, including steps that need to be taken to analyze the event, and the contents and timing of individual and regulatory notifications. This template is not designed to address all possible applicable requirements of these laws. If you experience a privacy or security incident, you should consult your own legal counsel to determine the specific requirements that will be applicable, given your particular situation.

that information, it is an unauthorized disclosure. These events are Security Breaches.
As part of the investigation, the Acme [Incident Response Team] will take immediate steps to close any open security gaps (such as isolating systems that may be compromised) and preserve evidence of what happened. The [Incident Response Team] will document the incident and take steps to recover the Personal Information (if possible) and obtain assurances from any unauthorized recipients that the Personal Information was not used and has been deleted. The [Incident Response Team] must prepare an incident summary along with root cause analysis (if applicable) and recommendations for the business. Any material recommendations must be communicated to [WHERE] for tracking and verification that the remedial steps have been taken.

All Security Breaches must be evaluated to determine the proper company response. This process applies to Acme's own Security Breaches as well as to Security Breaches that affect our vendors and service providers. Our contracts with our vendors require them to notify us of any Security Breaches that they experience.

Determine if the incident involves Acme client Personal Information. If client data is involved, the impacted client must be notified so that it can initiate its incident response processes. Notification must generally occur within 24 hours[2] of our determining that a Security Breach impacted client data.

Client notification are generally made by [WHO] as follows:
[ADD PROCESS]

Acme's contracts many impose additional obligations on Acme with regard to breaches involving client data.

Acme must provide the client with all of the information that the client reasonably needs to assess its obligations and mitigate risk. At minimum, Acme should provide the client with the details of the incident, including:

- The incident summary (or other description of what happened),
- The "root cause" analysis,
- A list of the individuals impacted (or other description of the impacted population),
- A list of the data elements impacted,
- Acme's analysis of the risk of harm presented by the incident along with a copy of the completed Incident Response Scorecard if the risk of harm is low,
- A description of the action(s) that Acme is taking to mitigate individual harm, and
- A description of the action(s) that Acme is taking to prevent a reoccurrence of the incident.

If Acme does not have all of this information available when the initial client notification is made, the information may be provided to be client as it becomes available. (For example, if Acme has inadvertently disclosed Personal Information to an unauthorized third party, Acme may obtain written assurances from the third party regarding its deletion of the data after the initial notification. Acme

[2] The GDPR standard is "without undue delay." Under the final WP29 Guideline, the controller becomes aware of when the processor informs it of the breach.

should inform the client when such assurances have been received. Acme may also provide additional information requested by the client, as may be reasonable given the nature of the breach.

Individual and regulatory notifications for breaches involving client Personal Information are the responsibility of the client. If the client requests that Acme make these notifications, Acme may (in its discretion) do so. Acme may also be contractually obligated to undertake notifications.

Acme may also ask for permission to make the notifications, such as when a Security Breach impacts multiple Acme clients and it would be more efficient for notifications to come from Acme. The Privacy Office will assist with making these requests.

Evaluate the Risk of Harm using the following 3-Step Process.

In responding to Security Breaches, it is essential that we quickly and accurately assess the risk of harm. If individuals are at risk of harm, Acme policy is to provide the appropriate notification as soon as possible so that we can help them mitigate the harm. If individuals are risk, we will provide notifications even if there is no specific legal obligation to do so. If individuals are not a real risk of harm, Acme policy is to provide notifications as may be required by law. We use a 3-step process to evaluate and document the possible risk of harm.

STEP 1: **Determine if there is a high risk to the impacted individuals as a result of the incident.**

If so, notification of individuals and (in some cases) the appropriate Regulatory Authority is required without undue delay.

Generally speaking, a breach creates high risk for an individual when, if unaddressed, such a breach is likely to have a significant detrimental effect on the individual – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Risk has to be assessed on a case by case basis, taking into account the circumstance of the incident and the nature of the Personal Information that has been compromised. For example, if sensitive data elements, such as bank account details, that could put someone at risk of financial crime are lost, there is high risk. Even less sensitive data elements, such as email addresses, may result in high risk, if the loss of the data element puts the individual at risk of phishing. On the other hand, the loss of a staff directory containing the types of data elements found on employee business cards, would not normally result in high risk. Similarly, if the personal information is strongly encrypted, and the encryption keys are not compromised, the incident will not result in high risk of harm.

As a matter of policy, we assume that a high risk of harm exists if unencrypted sensitive data is stolen. We also assume that a high risk of harm exists if sensitive personal information (such as national

identification numbers, tax identification numbers or financial account information) or Special Categories of Personal Data have been transmitted to an unknown or untrusted recipient.

If there is a high risk of harm, the following steps must be taken immediately: *Time is of the essence.*

1. Acme (or its client, as applicable) must notify the competent Regulatory Authority immediately. [This notice is made by the Chief Privacy Officer, the General Counsel or the Regional Data Protection Officer.] If applicable and appropriate, notification may also need to be made to (i) law enforcement, (ii) other regulatory agencies, (iii) PCI fraud teams, and (iv) the company insurance carrier.

2. Acme (or its client, as applicable) must notify the affected individual as quickly as possible.

    - The notification letter should alert individuals about the possible harm as well as steps that the individuals should take to minimize the risks.

    - The notification letters must fully comply with all applicable legal requirements, depending on the residency location of the data subject:

        a) describe the nature of the Security Breach including where possible, the date of the breach, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Information records concerned;
        b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
        c) describe the likely consequences of the Security Breach;
        d) describe the measures being taken to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

    - *If it not possible to send letters in a timely manner, Acme must consider other ways to making individuals aware of the high risk of harm. For example, Acme may post a notice regarding the incident on its website homepage and send information about the incident to individuals via email.*

    3. Acme should notify other authorities as maybe appropriate given the situation. For example, if data subjects are located in multiple countries, Acme may notify relevant data protection authorities in these countries so they can provide appropriate support to individuals as may be needed.

If there does not appear to be a high risk to the individuals, move to step 2.

STEP 2:	**Determine the level of possible risk to the impacted individuals.** **If a risk of harm exists, notification to the Regulatory Authorities is required within 72 hours (if feasible). Individual notifications will be made if requested by the Authorities.**

Use the Incident Response Scorecard attached below to evaluate the risk of harm based on established factors that determine the likelihood of risk if Personal Information have been compromised. If the score generated by Incident Response Scorecard is 4 or less, there is a low risk of harm to the individuals. (Move to Step 3.)

To complete this analysis, Acme must consider (1) the specific data elements that were exposed, (2) the countries of residence of the impacted individuals, and, if applicable, (3) the specific country laws or national guidance. [The company's Chief Privacy Officer or DPO will complete this analysis.]

If security, confidentiality or integrity of the Personal Information has been compromised (*i.e., the score is 5 or more)*, there is risk of harm. In this case, the following steps must be taken:

1. Acme (or its client, if applicable) must notify the competent Regulatory Authority within 72 hours if feasible.[3] [This notice is made by the Chief Privacy Officer, the General Counsel or the Regional Data Protection Officer.] If applicable and appropriate, notification may also need to be made to (i) law enforcement, (ii) other regulatory agencies, (iii) PCI fraud teams, and (iv) the company insurance carrier.

2. Upon instructions from the Regulatory Authority, Acme (or its client) may be required to notify the impacted individuals. If notification is required, the contents of the letter shall reflect the legal requirements noted above as well as any additional information recommended by the Regulatory Authority.

If the Incident has not compromised the security, confidentiality or integrity of Personal Information, move to step 3.

STEP 3:	**Document that there is no risk of harm to individuals that requires notification of Regulatory Authorities or Individuals.** **Maintain documentation regarding the investigation in accordance with Acme's document retention policy.**

1. When individual notifications are not required either to alert individuals to a real risk of harm or to comply with a legal notification requirement, Acme will not notify individuals of the incident.

    - Acme is committed to ensuring that individuals' interests are protected in connection with security incidents. Our policy is to notify regulators and individuals (and provide appropriate remediation) any time individuals are at any real risk of harm as a result of our mistakes – regardless of whether there is any legal obligation to notify them.

    - Acme is also committed to complying with applicable legal requirements, which sometimes require breach notification even when there is no risk of harm. We will always provide breach notification as required by law. We will cooperate with Regulatory Authorities, should they determine that notification is needed even if the risk of harm is moderate or low.

[3] If notification to the Authority is delayed, Acme must explain the reasons for the delay in its notification.

- Article 34 of the GDPR explicitly states that a notification does not need to be made when the risk to individual rights and freedoms is not "high". This Article reflects the public policy view that individuals should not be needlessly alarmed about events that have not and will not put them at risk of harm.

- When there is not a risk to individual rights and freedoms, there is no reason to send notification letters. Sending the letters will likely cause individuals to speculate that they are at risk of harm, as there is no other reason for the letter. It may also numb them to important notification letters, which puts them at greater risk of harm in the future.

- Should any person have any concerns about the security of his/her information, Acme will address those concerns.

2. Acme retains records of all privacy incident investigations for a minimum of five (5) years. Send copies of your documentation (including the completed Incident Response Scorecard and any notification letter templates) [to where] for retention.

Incident Response Scorecard Template

Acme evaluates all incidents to determine if there is a risk that Personal Information have been compromised or that individuals have otherwise been made vulnerable to risk of harm. We consider four factors that must be considered to determine the risk of harm.[4] These factors are:

1. The nature and extent of the Personal Information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the Personal Information or to whom the disclosure was made;
3. Whether the Personal Information was actually acquired or viewed; and
4. The extent to which the risk to the Personal Information has been mitigated.

Personal Information (PI) is defined as:

> Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
>
> Any information (alone or when used in combination with other information within Acme's direct control) that can be used to identify, locate or contact an individual, together with all information related to such Individual.
>
> Personal Information includes all Sensitive Personal Information (including Special Categories of Data) and other obvious information, such as person's name or email address, as well as less obvious information such as any Internet Protocol (IP) address or biometric data, if such data could possibly be associated with an Individual.
>
> Personal Information can be in any media or format, including computerized or electronic records as well as paper-based files.

Sensitive Personal Information (SPI) has been impacted. SPI are a subset of PI, which due to their nature have been classified by law or policy as deserving additional privacy and security protections. Sensitive Personal Information consist of:

- All government-issued identification numbers (including social insurance or similar numbers, driver's license numbers, passport numbers and national identification numbers),
- Individual financial account numbers (bank account numbers, credit card numbers, other information if that information would permit access to an Individual's financial account),
- Account login credentials (such as usernames and/or passwords),

[4] These factors are articulated in United State Federal law, in the breach notification rule promulgated by the Department of Health & Human Services. See 45 CFR §164.402. This Scorecard also considered the factors set forth in the EU Article 29 Working Party *Guidelines on Personal data breach notification under Regulation 2016/679.*

- Individual medical records, genetic information and biometric information, and health insurance information.

- Consumer reporting data, including employment background screening reports, and

- Data regarding EU-residents that are classified as "Special Categories of Data" under European laws and consisting of (a) race or ethnic origin, (b) political opinions, (c) religion, (d) trade union membership, (e) sex life or sexual orientation, and (f) physical or mental health, as well as (g) criminal charges or records related to criminal offenses and allegations of crimes.

The scorecard below enables us to assess the risk of harm to individual from a Security Breach. If you have any questions about this Scorecard, please contact [NAME]. This document should be attached to the [incident report file].

1. The nature and extent of the Personal Information involved, including the types of identifiers and the likelihood of re-identification:

0. Low Risk	1. Possible Risk	2. High Risk
PI but no SPI and/or low risk of association	PI associated with an individual (but no SPI)	Unencrypted SPI
For example: individual name associated with public information (postal address, company name or title) or demographic data **Any PI or SPI if encrypted (or hashed) using an industry standard encryption provided that the encryption keys are not compromised**	Individual name associated with any other types of Personal Information, such as email address or telephone number, purchase history, employment details or salary information	Government-issued identifiers Individual financial account numbers User Account credentials (email address and passwords, security questions/answers)

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN:_____

_____

_____

If the data are appropriately encrypted, the risk of the breach will be low regardless of the other factors. Document:
(1) Encryption standard used: _____
(2) Confirm "default" key was changed:_____
(3) Confirm keys not compromised:_____
(4) Confirm that encryption was effective (e.g., device was not in "sleep mode" or other unencrypted state):_____

_____

_____

2. The unauthorized person who used the PI or to whom the disclosure was made:

0. Low Risk	1. Possible Risk	2. High Risk
Trusted Recipient	Trustworthy Recipient	Untrusted Recipient
Acme Affiliate Current Acme Vendor Current Acme Client Current Acme Business Partner Government Agency **PI is encrypted, so no disclosure**	Third party with whom Acme does not have a contractual relationship, but who provides credible assurances that the data will not be misused (*e.g.*, a former vendor or client) A regulated entity, such as a financial institution, insurance company or healthcare provider	Unknown recipient (*e.g.,* public disclosure or loss of data) Recipients with known or suspected malicious intent (*e.g,* theft of data)

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN:_____

3. Whether the PI was actually viewed or acquired:

0. Low Risk	1. Possible Risk	2. High Risk
Not viewed or acquired	Viewed (or partially viewed) but not acquired	Acquired
Acme determines that file has been sent to the wrong recipient and retrieves the data prior to its being accessed Recipient reports receiving an incorrect file without viewing contents and deletes (or returns) the file without reading, copying or printing Lost device/media is recovered and forensic analysis indicates that it was not accessed **PI is encrypted so cannot viewed or acquired**	Recipient opens package or file but realizes that it has been incorrectly directed and deletes (returns or destroys) the file without using or further disclosing the information	Acme cannot recover the data from the recipient

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN:_____

4. The extent to which the risk to the PI has been mitigated:

0. Low Risk	1. Possible Risk	2. High Risk
Acme has good-faith reason to believe that that PI have not and will not be used, disclosed or retained.	Acme has good-faith reason to believe that that PI have not and will not be used or disclosed.	No mitigation
PI have been fully recovered. Trusted or trust-worthy recipient has provided credible written assurances that the data has not been used or disclosed and that no instance of the data has been retained. **PI was encrypted so no risk**	PI have been recovered from active recipient systems. Trusted or trust-worthy recipient has provided credible written assurances that the data has not been used or disclosed (but retention in back-ups may occur). The trusted or trust-worthy recipient has established program to protect similar information internally.	Acme does not have any assurances regarding use, disclosure or retention of the PI

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN: _____.

5. Any other factors or information which can assist in determining the risk of harm: *For example, if the breach involves particularly vulnerable individuals (such as children) the risk may be higher, even if the score is low. Similarly, if the breach involves only a small number of individuals who are difficult to identify from the data, the risk may be lower, even if the score is high.*

EXPLAIN:_____

C. Calculate Risk Assessment Score

Add the total risk assessment score points from factors 1-4 above.

Total score 7 or 8: The Security Breach puts individuals at real risk of harm. The Regulatory Authority and the impacted individuals must be notified as soon as possible.

Total score 5 or 6: The Security Breach creates a risk of harm. The Chief Privacy Officer [or DPO] should notify the appropriate Regulatory authority to determine if notification of data subjects is warranted. If

the incident includes data elements that trigger breach notification laws in the United States, notification will likely be required in some states as well.

Total score 4 or less: There is no or a very low risk of harm. Although you may have risk factors (such as sensitive PI on a stolen device), the probability of compromise must be low (such as if the data is encrypted). Risk may also be low if the data were viewed by a trusted third party with appropriate mitigation of the event.

Total Score: _____