RCW 42.56.590 Breach Assessment

(For State and Local Government)

When to use this form

Use this form to determine whether an incident is a breach that requires notification. Any unauthorized use or disclosure of Personal Information may be a breach that requires notification under the Washington state data breach notification law (RCW 42.56.590). The factors in the assessment help with the breach determination. Please note they are not a scoring system. Determinations should be made on a case-by-case basis based on the facts of a particular incident.

Notification requirements

Notice must be sent to impacted individual(s) within thirty calendar days after discovery of the incident. The law allows for some delays of notification. See below.* Details about how to provide notice are included in RCW 42.56.590(4-7).

If you have to notify more than 500 people, the law requires notification to the Washington state Attorney General's Office within thirty calendar days after the date of discovery.

Section 1 – Investigation Details

REFERENCE NUMBER	DATE FORM COMPLETED	NUMBER OF INDIVIDUALS AFFECTED

DATE DISCOVERED	DATE(S) OF INCIDENT
FORM COMPLETED BY	TITLE
OTHERS CONSULTED	NAME AND CONTACT INFORMATION IF THIRD PARTY INCIDENT

FINAL DETERMINATION

☐ Breach occurred; provide notification as required by RCW 42.56.590
☐ Not a breach; notification may be provided but is not required by RCW 42.56.590

Section 2 – Incident Summary

DESCRIBE THE INCIDENT AND THE NATURE OF INFORMATION THAT WAS POTENTIALLY COMPROMISED

Section 3 – Was the information secured?

Was the information secured, meaning encrypted in a way that meets or exceeds the national institute of standards and technology standards (NIST) or is otherwise unusable, unreadable, or indecipherable to the unauthorized person(s) who had access to the information? (If unsure, contact an information technology professional to determine if information was secure.)

□ Yes. **RCW 42.56.590 only applies to information that is not secured. Completing the rest of the assessment is optional.**

□ No. **Continue assessment.**

Section 4 – Was the information Personal Information?

What data elements were potentially compromised? Mark the elements involved in your incident:

□	First name (or first initial) and last name
	In combination with any one or more of the following:
□	Full or last four digits of social security number
□	Driver's license or Washington identification card number
□	Account number, credit or debit card number or any required security code, access code, or password that would permit access to an individual's financial account
□	Full date of birth
□	Private key that is unique to an individual and that is used to authenticate or sign an electronic record
□	Student, military, or passport identification number
□	Health insurance policy number or health insurance identification number
□	Information about medical history, health condition, or a health care professional's diagnosis or treatment
□	Biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual
□	User name or email address, together with a password or security questions and answers that would allow access to an online account (does not require first name and last name combination)

Other information involved:

Section 4.a

Did you mark the name *and* at least one other data element?

□ Yes. **The information is Personal Information. Continue to Section 5.**

□ No. **Continue assessment.**

Section 4.b

Does the information include a user name or email address, together with a password or security questions and answers that would allow access to an online account?

□ Yes. **The information is Personal Information. Continue to Section 5.**

□ No. **Continue assessment.**

Section 4.c

Does the information include at least one element that would enable a person to commit identity theft?

□ Yes. **The information is Personal Information. Continue to Section 5.**

□ No. **The information is not Personal Information. Continuing is optional.**

Section 5 – Exception for Good Faith Acquisition

Is the person who received or accessed information:

□ An employee or agent of the agency;

□ Within the scope of work; and

□ Acting in good faith;

□ With no further use or disclosure

If all four are satisfied, the incident does not require notification. Continuing is optional.

Otherwise, continue assessment.

Section 6 – Risk Assessment

An unauthorized use or disclosure is presumed to be a breach that requires notification. That presumption can be overcome if there is a low risk that the incident will create a risk of harm. Use the factors below to determine whether, on balance, there is a low risk that the incident creates a risk of harm.

1. Nature and extent of Personal Information involved, including types of identifiers and ability to identify individual:

□ **Low** Information is unlikely or unable to be usable to identify a person or commit identity theft.

□ **Moderate** Information could be used to identify individual but is not sensitive or specially protected.

□ **High** Information includes elements that could be used for identity theft, or records that are highly sensitive or personal, and are protected by heightened confidentiality laws.

Explanation:

2. Nature of person who acquired, accessed, used or received the Personal Information:

□ **Low** Limited or no risk of re-disclosure of information by recipient.
Examples: Employee of another agency or trusted contractor; recipient required by law to maintain confidentiality such as attorney or law enforcement; recipient subject to confidentiality laws and confirmed did not access data or returned data intact and did not retain copy.

□ **Moderate** Moderate or unknown risk of disclosure.
Examples: Unclear or unknown whether recipient accessed or retained data; recipient returned information; recipient not subject to confidentiality laws but acting in good faith.

□ **High** Severe risk of disclosure and recipient likely to re-disclose, sell or transfer data or is known to have used Personal Information for malicious purposes.
Examples: Acquisition was because of a criminal act including theft or hacking or information was obtained by a person with dishonest motives.

Explanation:

3. Risk that Personal Information was actually accessed or acquired or viewed by unauthorized individual:

□ **Low** No proof of access or acquisition of Personal Information. Would be difficult or unable to access Personal Information without sophisticated or extreme measures and individual had limited opportunity or ability to do so, or able to demonstrate lack of access through technical assessment.

□ **Moderate** Unknown whether access to Personal Information was acquired or Personal Information was acquired by a known individual in a manner that could be replicated. Technical assessment of access shows limited access or is inconclusive. Means to access data commonly known or available.

□ **High** Known or reported that access to Personal Information was acquired, used, sold, or further disclosed for malicious purposes.

Explanation:

4. Mitigation steps taken. (**See below for examples of mitigation that an agency may choose to take to address an incident.)

Remaining risk to Personal Information after implementation of mitigation steps:

□ **Low** All corrective actions have been taken and risk of future occurrences has been removed or reduced to acceptable level.

□ **Moderate** Some corrective actions have been taken but other reasonable steps cannot be implemented due to cost or other factors.

□ **High** Significant risk of continuing compromise of Personal Information remains despite mitigation.

Explanation:

5. Other factors considered:

Section 7 – Final Determination and Explanation

□ Incident is not reasonably likely to create a risk of harm. Notification is optional and is not required under RCW 42.56.590.

□ Incident is reasonably likely to create a risk of harm. Proceed with notification required by RCW 42.56.590.

Finding and Explanation:

*Exceptions to delay notification (beyond 30 days):

- Notice may be delayed at the request of law enforcement pursuant to RCW 42.56.590(3)
- Notice may be delayed as necessary to determine the scope of the breach and restore the integrity of an impacted system
- Notice may be delayed for up to 14 days to allow for translation of notice to primary language of impacted individual

**Examples of mitigation:

Adopt encryption technologies	Change or strengthen password requirements	Create/perform new/updated risk management plan or risk analysis.
Implement new technical safeguards	Implement periodic technical and nontechnical evaluations	Improve physical security
Train or retrain workforce members	Provide contractor with additional training on security requirements	Provide free credit monitoring
Revise contract terms	Revise policies and procedures	Sanction workforce members involved (including up to termination)
Take other steps to mitigate harm (e.g. confirm deletion of email, return or destruction of mis-mailed letter)		