Data Breach Management and Mandatory Notification Policy

Policy Number	101
Policy Category	Statutory
Date Adopted	15 June 2026
Resolution Number	CNL/26/053
Approval Authority	Council
Next Review Date	01 May 2030
Policy Version Number	1
Department	Corporate Services
Policy Owner	Governance Manager

PURPOSE

The purpose of this Policy is to establish a consistent and effective framework for Diamantina Shire Council's management of actual, suspected and Eligible Data Breaches in accordance with the *Information Privacy Act 2009* and the Mandatory Notification of Data Breach (MNDB) Scheme.

This policy outlines Council's approach to:

- identifying, assessing, containing and responding to data breaches;
- mitigating the risk of harm to affected individuals and Council;
- meeting legislative obligations relating to the notification of Eligible Data Breaches;
- ensuring appropriate governance, accountability and recordkeeping practices; and
- supporting continuous improvement in the protection and management of personal information.

Council is committed to protecting the privacy, confidentiality and security of personal information held by Council and to responding to data breaches in a timely, transparent and risk-based manner.

POLICY OBJECTIVES

- Ensure compliance with the *Information Privacy Act 2009* and the Mandatory Notification of Data Breach Scheme.
- Establish a consistent framework for identifying, managing and responding to data breaches.
- Reduce the risk of harm to affected individuals and Council.
- Ensure timely assessment and notification of Eligible Data Breaches.
- Promote awareness, accountability and continuous improvement in information handling practices.

COMMENCEMENT OF POLICY

Commencement date will be the date of approval.

SCOPE

This policy applies to all Councillors, employees, contractors, consultants, volunteers, work experience participants and any other persons performing work on behalf of Council.

This policy applies to all personal, confidential and sensitive information collected, stored, accessed, managed and disclosed by Council in any format.

HUMAN RIGHTS COMMITMENT

Council has considered the human rights protected under the *Human Rights Act 2019* (Qld) (the Act) when adopting and/or amending this policy. When applying this policy, Council will act and make decision in a way that is compatible with human rights and give proper consideration to a human right relevant to the decision in accordance with the Act.

POLICY STATEMENT

Diamantina Shire Council is committed to protecting the privacy, confidentiality and security of personal information held by Council.

Council recognises that data breaches may occur through human error, system failure, malicious activity, cyber security incidents or unauthorised disclosure.

This policy establishes Council's framework for responding to actual, suspected and Eligible Data Breaches in a timely, transparent and risk-based manner in accordance with the *Information Privacy Act 2009*.

Principles

Diamantina Shire Council is committed to managing data breaches in accordance with the following principles:

- Accountability – Council officers are responsible for protecting personal information and responding to actual or suspected data breaches.
- Transparency – Council will manage and communicate data breaches in an open, timely and transparent manner, consistent with legislative obligations.
- Risk-Based Approach – Council will adopt a risk-based approach when assessing and responding to data breaches, taking into consideration the likelihood and severity of harm.
- Legislative Compliance – Council will comply with the Information Privacy Act 2009 and the Mandatory Notification Scheme requirements.
- Continuous Improvement – Council will review data breaches, response activities and control measures to strengthen information management and reduce the risk of future breaches.

- Protection of Personal Information – Council is committed to protecting the privacy, confidentiality and security of personal information held by Council.
- Multidisciplinary Approach – Council will adopt a multidisciplinary approach when managing data breaches, involving appropriate governance, operational, legal, cyber security and executive resources where required.

Stage 1 - Preparation

Council will maintain appropriate governance systems, procedures and training to support the effective identification and management of data breaches.

Preparation activities include:

- employee awareness and training
- maintaining a Data Breach Response Plan
- integration with cyber security and incident management processes
- periodic testing and review of response processes
- maintaining appropriate recordkeeping practices
- ensuring appropriate escalation and governance arrangements are in place

Stage 2 - Identification of a Data Breach

Council recognises that data breaches may arise through human error, system failure, malicious activity, cyber security incidents, contractor actions or unauthorised disclosure of information.

A data breach may be identified internally or externally and may involve personal, confidential or sensitive information held by Council.

Examples of actual or suspected data breaches may include:

- emails containing personal information sent to an incorrect recipient;
- unauthorised access to Council systems or records;
- phishing, malware or ransomware incidents;
- lost or stolen devices, records or storage media;
- accidental publication of confidential information;
- inappropriate access to information by employees or contractors;
- unauthorised disclosure of information by third-party service providers;
- suspicious login activity or unauthorised account access;
- physical records being lost, misplaced or improperly disposed of.

Data breaches may be identified through:

- employee reporting;
- cyber security monitoring and alerts;
- complaints from affected individuals;
- notification from external agencies or contractors;
- audit activities;
- system monitoring or investigations;
- reports from members of the public.

Where an actual or suspected data breach is identified, it must immediately be escalated in accordance with this Policy.

Council recognises that not all cyber security incidents constitute a data breach. However, all cyber security incidents involving potential unauthorised access to information must be assessed to determine whether a data breach or Suspected Eligible Data Breach has occurred.

Where a data breach involves a contracted service provider or third party acting on behalf of Council, the incident must immediately be reported to Council and managed in accordance with this Policy and relevant contractual obligations.

Reporting a Data Breach

All actual or suspected data breaches must immediately be reported to the Governance Manager.

Employees must not independently assess whether a breach constitutes an Eligible Data Breach.

Upon notification, Council will undertake a preliminary assessment to determine the nature, scope and potential impact of the incident.

If the incident involves personal information and may result in serious harm, the Data Breach Review Team (DBRT) will be convened to assess the incident and determine whether it constitutes an Eligible Data Breach under the *Information Privacy Act 2009*.

Responding to a Data Breach

Council will respond to actual or suspected data breaches through the following stages:

1. Preparation
2. Identification
3. Containment and Mitigation
4. Assessment
5. Notification
6. Post-Breach Review and Remediation.

Some stages may occur concurrently depending on the nature and severity of the breach.

Stage 3 – Containment and Mitigation

Containing and mitigating a data breach will be prioritised by Council to minimise the risk of harm to affected individuals, Council operations and Council systems.

Council will take all reasonable and immediate steps to contain the breach, mitigate risks and prevent further unauthorised access, disclosure or loss of information.

Containment and mitigation actions may include:

- recovering or securing information;
- requesting deletion or return of information disclosed in error;
- isolating or shutting down affected systems;
- disabling compromised user accounts;
- resetting passwords or access credentials;
- revoking system access permissions;
- temporarily suspending affected business activities or processes;
- implementing temporary controls or monitoring measures;
- securing physical records or devices;
- engaging internal ICT and cyber security resources;
- engaging external cyber security, forensic, legal or privacy specialists where required;
- preserving evidence for investigation purposes;
- notifying relevant contracted service providers;
- implementing interim risk reduction measures.

Where a data breach involves information technology systems, Council's Systems Administrator and relevant ICT personnel will take immediate action to contain cyber security threats and minimise further compromise.

Where appropriate, Council may engage external specialists to assist with:

- cyber incident response;
- forensic investigation;
- legal advice;
- privacy assessment;
- communications management;
- remediation activities.

Council will consider:

- the nature and severity of the breach;
- the sensitivity of the information involved;
- whether the breach is ongoing;
- whether the information can be recovered;
- whether additional individuals may be affected;
- whether interim controls can reduce the likelihood of serious harm.

Containment and mitigation activities may occur concurrently with assessment and notification activities.

Stage 4 – Assessment

To determine what other steps are needed, an assessment of the type of information involved in the breach and the risks associated with the breach will be undertaken. Some types of information are more likely to cause harm if compromised (i.e. financial account information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list).

Given Council's regulatory responsibilities, release of case-related personal information will be treated very seriously. A combination of information will typically create a greater potential for

harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Where Council reasonably suspects an Eligible Data Breach may have occurred, Council will undertake an assessment in accordance with section 48 of the *Information Privacy Act 2009*. Where required, Council may extend the assessment period in accordance with section 49 of the Act.

Factors to consider:

- **Who is affected by the Data Breach?**
  Council will review whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected, and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

- **What was the cause of the Data Breach?**
  Council's assessment will include reviewing whether the breach occurred as part of a targeted attack or through human error or an inadvertent oversight.
  The assessment will aim to determine:
    - Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability?
    - What steps have been taken to contain the breach?
    - Has the data been recovered or erased by the recipient?
    - Is the data encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the Affected Individuals?**
  Council's assessment will include reviewing what possible use there is for the data and any likelihood of serious harm. This involves considering if the data includes personal information or health information. The harm that arises as a result of a data breach will be context specific and vary for each case.

  The assessment will aim to determine:
    - The kind of personal information
    - The sensitivity of the personal information
    - Whether the personal information is protected by one or more security measures, and if so the likelihood that any of those security measures could be overcome
    - The persons, or the kinds of persons, who have obtained, or who could obtain, the personal information
    - The nature of the harm likely to result
    - Who is in receipt of the information?
    - What is the risk of further access, use or disclosure, including via media or online?
    - If case-related, does it risk embarrassment or harm to a client and/or damage Council's reputation?

  Other relevant matters which may be taken into consideration are:
    - Combination of information types
    - The amount of time the information was exposed or accessible
    - The circumstances of the affected individuals

- The circumstances in which the breach occurred
- Actions taken by the agency to reduce the risk of harm following the breach

The Council assessment (see attachment 'A") will also include consideration of whether the data breach would be considered an eligible data breach and reportable under the MNDBS.

Stage 5 – Notification

Council recognises that timely and appropriate notification of an Eligible Data Breach can assist affected individuals to take steps to reduce or prevent potential harm.

Council will comply with the notification requirements under the *Information Privacy Act 2009* and the Mandatory Notification of Data Breach Scheme (MNDBS).

Where Council reasonably believes that an Eligible Data Breach has occurred, Council will notify:

- the Queensland Information Commissioner; and
- affected individuals, as soon as practicable, unless an exemption under the Information *Privacy Act 2009* applies.

Notification Exemptions

Prior to issuing notifications, Council will consider whether any exemption under the *Information Privacy Act 2009* applies to the notification requirements.

Council may also consider whether delaying notification is necessary where notification may:

- compromise an investigation;
- prejudice law enforcement activities;
- expose system vulnerabilities;
- increase the risk of further harm;
- interfere with containment or remediation activities.

Notification to Affected Individuals

Council will determine the most appropriate method of notification based on:

- the nature and severity of the breach;
- the number of affected individuals;
- available contact information;
- the likelihood of serious harm;
- operational and practical considerations.

Where reasonably practicable, affected individuals will be notified directly by:

- telephone;
- email;
- letter; or
- in person.

Where direct notification is not reasonably practicable, Council may undertake public notification in accordance with the *Information Privacy Act 2009*.

Notification Content

To the extent reasonably practicable, notifications may include:

- the date of the breach;
- a description of the breach;
- how the breach occurred;
- the types of personal information involved;
- the period of exposure or unauthorised access;
- actions taken by Council to contain and mitigate the breach;
- recommended steps individuals can take to reduce potential harm;
- information regarding privacy complaints and review rights;
- contact details for Council or the nominated contact officer;
- information regarding the right to lodge a complaint with the Queensland Information Commissioner.

Public Notification

Where direct notification to affected individuals is not reasonably practicable, Council may publish a public notification on Council's website in accordance with the Information Privacy Act 2009.

Public notifications will remain publicly available on Council's website for a minimum period of 12 months.

Council will maintain a Public Notification Register in accordance with legislative requirements.

Stage 6 – Post-Breach Review and Remediation

Following a data breach, Council will undertake a post-incident review to identify lessons learned, assess the effectiveness of the response and implement corrective actions to reduce the risk of recurrence.

The post-breach review process will consider:

- the cause and contributing factors of the breach;
- the effectiveness of containment and mitigation activities;
- the timeliness and effectiveness of notifications;
- whether legislative and policy obligations were met;
- whether existing controls were effective;
- opportunities for procedural or system improvements;
- whether additional employee training or awareness activities are required;
- whether policy, procedure or technical control updates are necessary;
- whether audit findings or compliance issues have been identified;
- whether risks should be reassessed or escalated within Council's Risk Register;
- whether external service provider arrangements require review.

Corrective and remediation actions may include:

- implementation of additional security controls;
- policy or procedural amendments;
- system upgrades or configuration changes;
- employee education and awareness activities;

- contractual amendments with service providers;
- updates to risk assessments or risk treatments;
- improvements to records management practices;
- internal audit reviews or assurance activities.

Council will maintain appropriate records relating to:

- the breach;
- investigations undertaken;
- assessment outcomes;
- notification decisions;
- remediation activities; and
- lessons learned.

Where appropriate, Council may use outcomes from post-breach reviews to:

- improve governance controls;
- strengthen cyber security measures;
- improve privacy and information management practices;
- inform future training programs; and
- support continuous improvement activities.

Breaches relating to external service providers

Council recognises that external contracted service providers may collect, store, access, manage or process information on behalf of Council as part of delivering services or systems.

Council will endeavour to ensure contractual arrangements with service providers contain mandatory data breach reporting, cooperation and notification provisions, including obligations relating to:

- the protection and secure handling of Council information;
- immediate notification of actual or suspected data breaches;
- cooperation with Council investigations and response activities;
- implementation of containment and remediation measures;
- compliance with applicable privacy and information security obligations;
- participation in investigations, audits or reviews where required.

Where a data breach involves an external service provider, the provider must immediately notify Council upon becoming aware of an actual or suspected data breach involving Council information.

Council will work collaboratively with contracted service providers and relevant third parties to:

- contain and mitigate the breach;
- assess risks and potential harm;
- support investigation and remediation activities;
- determine notification obligations;
- minimise impacts to affected individuals and Council operations.

Any data breach involving a contracted service provider that impacts Council information, systems or operations must immediately be escalated to the Data Breach Review Team (DBRT).

Council may require external service providers to provide:

- incident reports;
- forensic investigation outcomes;
- remediation plans;
- evidence of corrective actions;
- confirmation of containment activities.

Where appropriate, Council may review:

- contractual arrangements;
- vendor security controls;
- compliance obligations; and
- ongoing suitability of service providers following a data breach incident.

Training and awareness

Council is committed to ensuring employees, contractors and relevant stakeholders understand their obligations regarding the protection, handling and management of personal information.

Council will provide training and awareness activities to assist employees in:

- identifying actual or suspected data breaches;
- understanding obligations under the *Information Privacy Act 2009* and the Mandatory Notification of Data Breach Scheme;
- recognising cyber security and privacy risks;
- appropriately escalating and reporting incidents;
- reducing the risk of human error data breaches.

Training and awareness activities may include:

- induction training for new employees;
- periodic refresher training;
- targeted role-specific training;
- cyber security awareness campaigns;
- phishing awareness and simulation activities;
- updates regarding emerging privacy or cyber security risks;
- guidance materials, procedures and awareness communications;
- lessons learned from data breach incidents or investigations.

Role-specific training may be provided to employees with elevated privacy, cyber security, governance or information management responsibilities, including:

- Executive Leadership Team members;
- Governance personnel;
- Information technology personnel;
- Records management personnel;
- employees managing sensitive or high-risk information.

Council may periodically review and test employee awareness and response capability to support continuous improvement in data breach prevention and response practices.

This Policy will be made available to employees and published on Council's website where appropriate.

Mandatory Notification of Data Breach Scheme Compliance

Council will comply with the requirements of the Mandatory Notification of Data Breach Scheme (MNDBS) under the *Information Privacy Act 2009*.

Where Council becomes aware of an actual, suspected or Suspected Eligible Data Breach involving personal information, Council will take reasonable steps to:

- identify and contain the breach;
- assess the breach in accordance with legislative requirements;
- mitigate the risk of harm to affected individuals;
- determine whether the breach constitutes an Eligible Data Breach;
- undertake notification obligations where required.

In accordance with sections 48–54 of the *Information Privacy Act 2009*, Council will:

- undertake an assessment where there are reasonable grounds to suspect an Eligible Data Breach may have occurred;
- complete the assessment within the legislated timeframe, unless an extension is permitted under the Act;
- take reasonable steps to contain and mitigate harm during the assessment process;
- notify the Queensland Information Commissioner where an Eligible Data Breach is confirmed;
- notify affected individuals where required under the Act;
- maintain records relating to Eligible Data Breaches and notification activities.

Council may also seek advice or assistance from the Queensland Information Commissioner where appropriate.

Council will manage Eligible Data Breaches in a timely, transparent and risk-based manner consistent with privacy, governance and public sector accountability obligations.

Internal Notifications

The Data Breach Review Team (DBRT) will be notified of all actual or suspected Eligible Data Breaches and significant data breach incidents.

The Chief Executive Officer will be notified where a data breach:

- involves a significant volume of personal or sensitive information;
- is likely to result in serious harm to affected individuals;
- involves health, financial or identity information;
- impacts children, vulnerable persons or at-risk individuals;
- involves critical infrastructure, essential systems or operational disruption;
- involves ransomware, cyber-attack, phishing, malware or unauthorised system access;
- has the potential to attract media, regulatory or public interest;
- may result in legal, financial or reputational impacts to Council;
- involves external service providers or third-party systems;
- may require notification to insurers, regulators or law enforcement agencies.

Where appropriate, Council may also notify:

- Council's insurers;
- legal advisors;
- cyber security specialists;
- law enforcement agencies;
- relevant government agencies;
- external service providers;
- communication or media representatives.

Internal notifications and escalation activities will be undertaken in a timely manner to support:

- containment and mitigation activities;
- legislative compliance;
- operational continuity;
- coordinated communications;
- risk management and governance oversight.

Significant data breaches may also be reported through Council's enterprise risk management, business continuity, cyber security or incident management frameworks where appropriate.

Data Breach Documentation

Documentation relating to data breaches will be stored in Council's document management system. Council will maintain an internal register of eligible data breaches. Council will also maintain a Public Notifications Register. This information is available on the Council's website for 12 months following a public notification of a data breach.

All records relating to data breaches will be managed in accordance with the *Public Records Act 2023* and Council's Records Management Framework.

Responsibilities

All employees will:

- follow the requirements of this policy and understand their obligations to minimise data breaches
- immediately report any actual or suspected data breaches via email to admin@diamantina.qld.gov.au

The Data Breach Review Team will:

- review, assess and remediate incidents escalated to the team
- follow this policy when responding to a data breach
- evaluate the associated risks
- consult with internal and external stakeholders as required
- determine if a data breach is an eligible data breach
- review and respond to data breaches impacting Council's external service providers.
- follow up on containment actions
- determine recommendations to prevent a repeat incident
- prepare and send internal notifications

The Systems Administrator will:

- take immediate and any longer-term steps to contain and respond to security threats to Council's IT systems and infrastructure

The CEO will:

- oversee significant or high-risk breaches
- ensure appropriate resourcing
- support organisational response activities

The Governance Manager will:

- forward each data breach incident to the DBRT, which may include a recommendation to consider the incident as an eligible data breach
- Will convene the DBRT when in receipt of an actual or suspected data breach for assessment and determine if the affected Individuals should be notified
- undertake notifications as required to affected Individuals and the Queensland Information Commissioner, including any eligible data breaches
- prepare a data breach incident report for each separate data breach incident
- notify Council's insurers as required
- maintain public notification register
- coordinate OIC liaison

Complaints

Any complaints in relation to a decision or a service relating from this policy will be assessed and managed in accordance with Council's Administrative Action Complaints Policy, a copy of which can be found on Council's website.

When an individual feels that they are the subject of Council's failure to act compatibly with human rights, they can make a complaint directly to Council. These complaints will be assessed against the *Human Rights Act 2019*.

Complaints may be made as follows:
In writing to:
Chief Executive Officer
Diamantina Shire Council
17 Herbert Street
BEDOURIE QLD 4829

Via email – admin@diamantina.qld.gov.au

DEFINITIONS

Term	Definition
Affected Individual	An affected individual under section 47(1)(ii) of the *Information Privacy Act 2009*.
Contracted Service Provider	An external entity engaged by Council to provide services involving the collection, storage, management, processing or access to Council information or systems.
Council	Diamantina Shire Council
Cyber Security Incident	An event or activity that compromises, or may compromise the confidentiality, integrity or availability of Council's information, systems, networks or technology assets.
Data Breach	The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
Data Breach Response Plan	A more detailed procedural document complementing the Data Breach Policy, which could be an internal document detailing the agency's more specific processes in managing and responding to a data breach.
Data Breach Review Team (DBRT)	Comprises the following officers: • Director Corporate Services • Governance Manager • Systems Administrator
Eligible Data Breach	An "Eligible Data Breach" will have occurred under section 47 of the IP Act where: (a) there has been unauthorised access to, or unauthorised disclosure of personal information held by an agency, and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or (b) there has been loss of personal information held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and the loss is likely to result in serious harm to any of the individuals to whom the information relates.
ELT	Executive Leadership Team
Employees	Any person who is an employee of Council (permanent, part-time and/or casual), volunteers, work experience contractors and consultants.
IP Act	*Information Privacy Act 2009*
Personal Information	Information or an opinion about an individual or an individual who is reasonably identifiable from the information or opinion:

Term	Definition
	(a) whether the information or opinion is true or not, and (b) whether the information or opinion is recorded in a material form or not.
Public Notification	A notification provided under s53(2) of the IP Act when any or all of the Affected Individuals by an Eligible Data Breach are unable to be notified individually.
Public Notification Register	A register maintained by Council containing public notifications relating to Eligible Data Breaches in accordance with the *Information Privacy Act 2009*.
Sensitive Information	Information and data (including metadata) including personal information, information protected under legal privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans or significant buildings, Security Classified Information and information related to Council's IT/cyber security systems.
Serious Harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or (b) serious harm to the individual's reputation because of the access or disclosure.
Suspected Eligible Data Breach	A data breach where there are reasonable grounds to suspect that the breach may constitute an Eligible Data Breach under the *Information Privacy Act 2009*, pending assessment or investigation.
Unauthorised Access	Includes: • an Employee browsing customer records without a legitimate purpose • a computer network being compromised by an external attacker resulting in Sensitive Information being accessed without authority.
Unauthorised Disclosure	Includes: • an Employee sending an email containing personal information to the wrong recipient • incorrect contact details entered into automatic information systems e.g. rates notices

SUPPORTING DOCUMENTATION

Legislation	*Information Privacy Act 2009*
Council Policies	Procurement Policy Records Management Policy Queensland Privacy Principles (QPP) Privacy Policy Cyber Security Policy (to be drafted)
Council Delegations	N/A
Council Forms	MNDB Notification
Supporting Documents	Corporate Plan 2022 – 2027 Mandatory Notification of Data Breach Procedure Data Breach Response Plan Business Continuity Plan Disaster Recovery Plan Eligible Data Breach Register

VERSION CONTROL

Version	Adopted	Comment	eDRMS #
1	15 June 2026	Resolution: CNL/26/053	330501

Annexure A – Process for Identifying Mandatory Notification of Data Breach

Process for identifying Mandatory Notification of Data Breach (MNDB) scheme obligations (For initial consideration and s.48 assessments)

A data breach has occurred, does it involve personal information?

Yes / **No** → MNDB scheme obligations do not apply

MNDB scheme obligations may apply

Gather information and determine the likelihood of serious harm, having regard to:

- The kind of personal information
- The sensitivity of the information
- Is information protected by one or more security measures?
- The likelihood measures could be overcome
- Persons (or kinds), who have obtained, or who could obtain, the personal information
- The nature of the harm likely to result from the data breach
- Depending on the circumstances, any other relevant matters, like how long information was exposed, circumstances of affected individual, how it occurred, combinations of personal information and actions taken by agency to reduce the risk of harm.

Determine knowledge, suspicion or belief of EDB and relevant obligations

Does the information indicate and/or support an Eligible Data Breach (EDB)?	Eligibility	Scheme obligations		
		Contain and mitigate	Assess	Notify
Evidence indicates only a **possibility**, (**note**: you may need to seek more information and consider containment)	Possibility			
Some evidence supporting notion of EDB. Not enough for belief, but **more than a possibility**	Reasonable suspicion	✓	✓	
Sufficient evidence to accept the notion that the breach is eligible, as opposed to rejecting it	Reasonable belief	✓		✓
Knowledge that an EBD has occurred	Knowledge	✓		✓