National Storage Financial Services Limited

Incident and Breach Policy

Adopted: 29 September 2021

Reviewed: 22 June 2022

Contents

1. Section 1 Overview 3

2. Section 2 Responsible persons and contact points 6

3. Section 3 Identification and Classification of incidents and breaches 7

3.1 Operational Risk Incidents 7

3.2 Regulatory and Compliance Incidents 7

3.3 Determining a Breach 8

3.4 What is a Likely Breach 8

3.5 Significant Breaches 8

3.6 Other Regulatory Breaches 9

Privacy Law – Notifiable Eligible Data Breaches 9

4. Section 4 Escalating and Reporting Incidents 10

4.1 Reportable Breaches 10

4.2 Investigations into a Breach 12

4.3 Other Reportable Situations 12

4.4 Reportable Situations about Other Licensees 12

4.5 Assessment and Rectification of Breaches/Incidents 12

4.6 Non-reportable Breaches 13

5. Section 5 Incident and Breach Register 13

6. Section 6 Policy Owner, Review and Version Control 13

Section 1 Overview

Purpose

National Storage Financial Services Ltd (ACN 600 787 246) (**National Storage**) recognises that prompt identification and resolution of incidents and breaches is critical to ensure any material gaps and issues in its control environment are identified, escalated and rectified in a timely manner and in accordance with this Policy. As such, National Storage and the National Storage Group are committed to the timely management and remediation of all incidents and breaches and this Policy requires that all staff are to be aware of and escalate any suspected or actual breaches of internal policies and procedures, external rules and regulations, as well as any operational incidents.

This Policy is also intended to assist in minimising client and reputation impacts and that we have addressed any internal and external disclosure requirements. By understanding and addressing the underlying cause of an incident or breach, this helps to minimise the potential for recurrence.

National Storage is subject to legal and regulatory obligations in relation to incident and breach requirements. This includes the obligation to report certain breaches to regulators as required by law. It is a legal requirement that National Storage Financial Services Limited as a holder of an Australian Financial Services Licence (**AFSL**) (AFSL No. 475228) must establish and maintain compliance measures that ensure, as far as is reasonably practicable, the licencee complies with the provisions of the financial services laws at all times.

The purpose of this Policy is to ensure that there is an appropriate and effective framework for the identification, management, escalation, resolution and reporting of incidents, breaches, and potential breaches.

Application

This Incident and Breach Reporting Policy (**Policy)** covers the following:

- National Storage Group employees;
- National Storage Group directors; and
- any other person acting on behalf of National Storage such as a contractor.

Related Policies and Procedures
Risk Management Policy
Anti-Bribery and Corruption Policy
Privacy Policy
Client Complaints Handling Policy
Code of Conduct
AML/CTF Program
All Policies where there is a requirement to report breaches or incidents, as those breaches or incidents should be reported in accordance with this Policy.

Definitions

Term	Definition
AFSL	Australian Financial Services Licence
AML/CTF	Anti-Money Laundering and Counter-Terrorism
ASIC	Australian Securities & Investments Commission
AUSTRAC	Australian Transaction Reports and Analysis Centre
Board	The board of directors of National Storage Financial Services Limited
CEO	Chief Executive Officer
CFO	Chief Financial Officer
Corporate Authorised Representative	A company appointed by an AFSL holder to be an authorised representative of that AFSL holder to provide financial services on its behalf and/or under its authority.
Corporations Act	*Corporations Act* 2001 (Cth)
Head of Legal and Governance	Also being the Executive Director, Company Secretary, Compliance Officer, and Risk Officer.

National Storage or National Storage Group	National Storage Financial Services Limited (**National Storage**), AFSL No. 475228 (**Licensee**), as Responsible Entity for the following 2 named registered managed investment schemes: • National Storage Property Trust (ARSN 101 227 712); and • National Storage Active Investment trust (ARSN 609 004 837) Any corporate authorised representative of National Storage.
OAIC	Office of the Australian Information Commissioner
Related Body Corporate	Has the meaning given by section 50 of the Corporations Act being: ▪ a holding company of another body corporate; ▪ a subsidiary of another body corporate ▪ a subsidiary of a holding company of another body corporate. Applying this definition to joint ventures and/or partially owned companies can be a complex exercise. If there is any doubt as to whether a company is a Related Body Corporate, the issue should be escalated to the Head of Legal and Governance. *Note that a conflict of interest may still be present even if the relevant company falls outside this definition*

Relevant Legislation / Regulation	**Jurisdiction**
Corporations Act 2001	Cth
ASIC Regulatory Guide 78: Breach reporting by AFS licencees and credit licencees	Cth
ASIC Regulatory Guide 104: AFS licensing: Meeting the general obligations	Cth
Privacy Act 1988	Cth
Anti-Money Money Laundering and Counter Terrorism Financing Act 2006	Cth

Section 2 Responsible persons and contact points

Any staff who has identified an incident has responsibilities under this Policy to escalate and report the incident immediately as described in section 4 below.

The persons with primary responsibility for the application and compliance with this Policy are:

- the CEO; and
- Head of Legal and Governance/Incident Owner for the purposes of monitoring, actioning, and closing the incident.

The Head of Legal and Governance is responsible for:

- Ensuring that each business has implemented adequate processes to identify, manage and report incidents in a timely manner;
- Reviewing all incidents and associated actions to ensure all relevant details and necessary actions have been reported and actioned, including in a timely manner;
- Liaising with the CEO in determining whether an incident needs to be reported internally or externally, for example to regulators or investors;
- Prepare the breach reports, engaging with business representatives and circulating to relevant stakeholders for their input prior to finalising;
- Lodge breach reports with regulators and manage any subsequent correspondence or discussions;
- Ensuring employees are aware of this Policy and any updates, including that they understand this Policy;
- Ensuring incident and breach reporting is included in Board reporting.

The business representative with responsibility for reporting an incident needs to:

- Undertake best endeavours to identify and escalate high-risk and significant incidents within 24 hours;
- Complete the incident template and gather and include all relevant information, data and any financial information in a timely manner including the recommended actions to mitigate the risk of the incident re- occurring; and
- Assist with the assessment of the incident, particularly if it is being assessed for "significance".

The Head of Legal and Governance will:

- Assist with identifying information which may need to be gathered for the investigation of an incident;
- Determine if legal professional privilege should be claimed and if so, implementing;
- Review the incident and the information gathered;
- Advise whether the incident is a breach of law;
- Manage any external advice obtained; and
- Liaise with senior management to determine whether the breach is significant.

Section 3 Identification and Classification of incidents and breaches

All incidents should be escalated and reported in accordance with this Policy and the two main types of incidents covered by this Policy are:

- Operational risk incidents; and
- Regulatory and compliance incidents.

3.1 Operational Risk Incidents

For the purpose of this Policy, an operational risk incident is an incident caused by inadequate or failed internal processes, people, and systems or due to external circumstances. Examples include:

- payment or accounting error e.g., paying the same invoice twice or where financial accounts have been over-stated or under-stated due to a breakdown in internal controls or due to human error;
- allocating a product to an investor which is inconsistent with their investment instructions or allocation preference;
- investor correspondence including marketing materials and presentations sent containing errors or omissions;
- investor information is compromised, due to a cyber security issue, which causes a breach or incident in relation to the privacy policy;
- errors caused by external service providers;
- non-compliance with an internal policy and/or procedure which does not represent a breach of any other requirements;
- an operating incident which does not constitute a breach of other regulatory or legal obligations or ASIC related documents (constitution or compliance plans); or
- where the cause of an incident is a departure from standard procedures by a third party such as a broker, client, custodian, administrator, supplier, or other actions by an external third party.

An incident may expose:

- underlying control weakness, such as an inadequacy or absence of an accounting, financial, operational, policy or other control within National Storage Group;
- matters considered likely to attract adverse publicity

3.2 Regulatory and Compliance Incidents

Regulatory and compliance incidents include some of the following:

- Actual, potential, or suspected breaches of legal or regulatory requirements, or an incident which will impact our ability to meet client, regulator, market, contractual or management expectations, or which impacts our ability to meet legal or regulatory requirements;
- Material exceptions to internal policies;
- Any improper, unlawful, or unethical behaviour or action which may have a negative impact for the National Storage Group, our clients or counterparties or the markets in which we operate;
- An incident that may or will impact the Group's reputation internally or externally.

Some examples of regulatory and compliance incidents include:

- Non-compliance/breach of provision(s) in a Constitution of any company or fund which form part of the National Storage Group;
- Non-compliance/breach with the Corporations Act or any other financial service laws;
- Non-compliance/breach with other legal and regulatory requirements, such as Anti-Money Laundering and Counter-Terrorism legislation, Privacy legislation etc... and
- Non-compliance with the conditions of the National Storage Financial Services Limited's AFS Licence.

3.3 Determining a Breach

In some jurisdictions in which we operate there may be legal or regulatory requirements to report certain types of incidents. There may also be a requirement to report certain incidents due to contractual obligations.

The Head of Legal and Governance needs to decide as to whether there has been a potential breach of the law or if it is likely that there will be a breach of the law in the future. Consideration should be given to engaging other relevant stakeholders.

For breaches, the Head of Legal and Governance, together with the CEO, will jointly be involved in the investigation and decision making in connection with any breach reporting obligations.

3.4 What is a Likely Breach

An AFSL holder must report not only when it breaches an obligation, but also when it is "likely to breach" an obligation.

For the purposes of this document, 'likely breach' involves the entity becoming aware that it is no longer able to comply with the obligation, i.e., it is not presently in breach but will certainly breach.

The determination of significance will be actioned by the Head of Legal and Governance.

Examples of likely breaches include, but are not limited to:

- an incident that potentially could be a breach;
- a situation which is currently under investigation; or
- if cash flow forecasting is showing that the RE is no longer able to meet cash requirements as prescribed under the AFSL.

3.5 Significant Breaches

A licencee does not have to report all breaches or likely breaches, only those that are "***significant***".

There are two ways to determine whether a breach (or likely breach) is significant:

(a) Deemed significant breaches – certain types of breaches are taken to be significant; and

(b) Other breaches that may be significant – National Storage will need to assess whether the breach (or likely breach) is significant in consideration of the factors in s912D(5) of the Corporations Act.

Deemed significant breaches include breaches:

- that constitute the commission of an offence which is punishable by a penalty that

may include imprisonment for three months or more if the offence involves dishonesty or 12 months or more in any other case;

- of a civil penalty provision (except where excluded by the regulations);
- misleading or deceptive conduct; or
- that result, or are likely to result, in material loss or damage to clients or to members of a managed investment scheme or superannuation entity.

If the breach (or likely breach) is not a deemed significant breach, National Storage will need to assess the significance of the breach (or likely breach) having regard to the following factors, as listed in s912D(5) of the Corporations Act:

- the number or frequency of similar breaches;
- the impact of the breach or likely breach on the licencee's ability to provide the financial services covered by the licence;
- the extent to which the breach or likely breach indicates that the licencee's arrangements to ensure compliance with those obligations is inadequate; and
- any other matters prescribed by current Regulations.

Some examples of breaches that ASIC considers may be significant and consequently reportable are:

- a failure to maintain professional indemnity insurance;
- a failure to prepare cash flow projections;
- a failure to detect previous breaches; and
- regular occurrences of representatives giving inappropriate advice.

3.6 Other Regulatory Breaches

This is a category of Breaches created for the purposes of this Policy, and means a breach of other applicable regulations, which may be required to be reported to a particular regulator, other than ASIC. Examples of such breaches are:

- Breaches of the Privacy law and Regulations which require reporting to the OAIC; and
- Breaches of the AML/CTF Legislation which require reporting to AUSTRAC.

Privacy Law – Notifiable Eligible Data Breaches

A Breach that is assessed to be an "***eligible data breach***" must be notified to the OAIC and the affected individual(s) as soon as reasonably practicable after such assessment is made.

An assessment of whether a privacy law breach is an "***eligible data breach***" must be completed within thirty (days, from the first day the breach is first identified.

An "***eligible data breach***" is a breach in which the following criteria are satisfied:

- there is unauthorised access or unauthorised disclosure of personal information, or there has been a loss of personal information;
- there is a likely result of "***serious harm***" to the affected individuals; and
- we have not been able to prevent the likely risk of the serious harm with any remedial action.

In determining if the affected individual(s) have experienced "***serious harm***" or there is "***likely to be serious harm***", the following factors may be considered.

(i) The kind or kinds of information;

(ii) The sensitivity of the information;

(iii) Whether the information is protected by one or more security measures;

(iv) Where the information is protected by a security measure, the likelihood that any of those measures could be overcome;

(v) The persons, or the kinds of persons, who have obtained, or could obtain, the information;

(vi) The nature of any harm;

(vii) If a security methodology or technology:

a. Was used in relation to the information; and

b. Was designed to make the information unintelligible or meaningless to persons not authorised to obtain the information;

(viii) The likelihood that the persons, or kinds of persons, who:

a. Have obtained, or who could obtain, the information, and;

b. Have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

c. Have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;

(ix) Any other relevant matters.

Section 4 Escalating and Reporting Incidents

All Breaches and Incidents must be recorded and reported internally at first instance.

Where you become aware of an incident or breach, please immediately contact the Head of Legal and Governance and / or your department manager. Failure to report an incident or significant unexplained delays in reporting an incident may result in escalation to the staff member's manager, CEO, and the Human Resources Department to determine whether any disciplinary action is required to be taken, including formal warnings or termination of employment agreement.

For suspected frauds, please refer to Anti Bribery and Corruption Policy.

Reporting of any incident or breach should be done via the standardised template that will be completed by the staff member who identifies the breach or incident. The completed template must be forwarded to the Head of Legal and Governance for their review and assessment.

Any significant or high-risk incident must be escalated to the CEO within 24 hours of detection. This can be done via email with relevant details that the staff member is aware of.

However, certain breaches such as significant breaches and eligible data breaches are required to be reported to the relevant Regulators. These are dealt with under the section Reportable Breaches below. All other Breaches and Incidents will be dealt with as described under the section Non-reportable Breaches.

For all reportable breaches to ASIC or any other reportable matters to relevant regulators, the Head of Legal and Governance must escalate the matter to the Board, the CEO, and the CFO. These stakeholders should be included in the review of the draft notices.

4.1 Reportable Breaches

A Reportable Breach will be determined by the Head of Legal and Governance who may also consult the CEO and seek clarification from senior management before finalising the

decision. Based on the nature and type of breach or incident, different reporting requirements may need to be followed, including having to meet different reporting requirements of the various Regulators.

Financial Services Laws & ASIC Breach Reporting.

A Significant Breach (including Likely Breach) must be reported to ASIC as soon as practicable and in any case within 30 days after becoming aware of, or are reckless with respect to whether, there are reasonable grounds to believe a breach or likely breach has arisen.

ASIC deems that an AFSL holder becomes aware of a breach (or likely breach) when the person responsible for Compliance becomes aware of, or is reckless with respect to whether, there are reasonable grounds to believe the breach or likely breach has arisen.

It is important that National Storage report significant breaches to ASIC as early as possible, even where information may still be being gathered to analyse the root cause or identify potential remedies.

Failure to report a significant breach within the prescribed timeframe is an offence and may result in penalties. It is also a Significant Breach in itself.

Where the Head of Legal and Governance determines that the breach is significant or where there is a breach which is a notifiable Regulatory Breach, they will immediately and no later than within 30 days:

(i) notify all members of the Board as appropriate, including the CEO and the CFO;

(ii) notify the AFSL Auditor (where the breach relates to AFSL Conditions);

(iii) complete a breach report which follows ASIC's RG 78 or any other relevant guidance provided by ASIC); AFSL holders need to submit breach reports to ASIC via the ASIC Regulatory Portal. The portal replaces the previous paper submission processes. Submitting breach reports via online forms on the portal features mandatory fields designed to help licencees comply with their breach reporting obligations. There are no changes to the ongoing breach reporting obligations for AFS licencees as a result of this change.

(iv) undertake the task of reporting the breach to ASIC or the relevant regulator with the assistance of a legal advisor and/or AFSL Auditor as required; and

(v) keep the Board updated as to the progress of the matter including the CEO and the CFO.

(vi) All breaches will be reviewed at Board level until such breach has been closed by the relevant regulator.

Eligible Data Breach Notifications

Where a privacy breach is held to be an 'eligible data breach", the breach must be reported and notified to both of the following:

- The OAIC; and
- The affected individual(s).

The notification to both parties identified above must be made as soon as practicable after it has been determined on reasonable grounds that there has been an "eligible data breach".

The Head of Legal and Governance, in consultation with relevant senior management where so required, will assess if the data breach is one that is "eligible" and hence triggering the notification requirements.

Such assessment must be completed within thirty (30) days from the date the breach is identified and there are reasonable grounds to suspect that the breach is an eligible data breach.

Breach reports relating to personal data must be in the prescribed format.

4.2 Investigations into a Breach

Investigations into whether a significant breach (or likely significant breach) has occurred, which continue for a period of more than 30 days, must be immediately notified to ASIC on the 31st day.

4.3 Other Reportable Situations

In addition to significant breaches (or likely breaches) and investigations, additional reportable situations must be reported to ASIC, regardless of whether they are significant. Additional reportable situations include where National Storage or its representative:

- Engages in conduct constituting gross negligence in the course of providing a financial service; or
- Commits serious fraud.

Such other reportable situations must be reported to ASIC within 30 days of first becoming aware of, or are reckless with respect to whether, there are reasonable grounds to believe the situation has occurred.

4.4 Reportable Situations about Other Licensees

From October 2021, National Storage is also obliged to report to ASIC if it has reasonable grounds to believe that a significant breach (or likely significant breach) or additional reportable situation has arisen in relation to another AFS licencee involving personal advice to retail clients about relevant financial products.

Reportable situations about other AFS licencees must be reported to ASIC within 30 days of first becoming aware of, or are reckless with respect to whether, there are reasonable grounds to believe the situation has occurred.

4.5 Assessment and Rectification of Breaches/Incidents

Each breach must be assessed on its individual facts and surrounding circumstances. In some circumstances breaches/incidents will be able to be rectified. The rectification action taken will be determined by the Head of Legal and Governance (and if required CEO or Board) having regard to the nature of the breach and the circumstances surrounding the breach, as follows:

(i) Carrying out an analysis of how or why the breach/incident occurred;

(ii) Assessing the impact on the client (if any) and how this will be managed, documented, and remediated;

(iii) Initiating appropriate action and providing relevant training (if appropriate) for the personnel responsible for or working in the area within which the breach/incident occurred;

(iv) Notifying the Board on any training or action initiated to prevent the recurrence of the breach/incident;

(v) Carrying out an internal review on the area where the breach occurred within three months of the action taken and any training having been provided to determine

whether the rectification action has been successful in preventing further breaches/incidents.

(vi) Notifying the Board of the outcome of the internal review undertaken.

(vii) Continuing the review process if the Board is not satisfied with the result of the internal review.

4.6 Non-reportable Breaches

For non-reportable breaches, the requirements as outlined in this Policy apply.

Section 5 Incident and Breach Register

Incidents must be reported and finalised as soon as possible by completing the Incident Reporting template ("incident template"). The incident template should be completed and sent to the Head of Legal and Governance no later than 10 days from detection. The Head of Legal and Governance should complete the review and assessment and approve the incident within 30 days from detection.

The Incident Reporting template sets out the information that needs to be provided by staff in reporting the incident and the assessment which needs to be undertaken by the Head of Legal and Governance.

Section 6 Policy Owner, Review and Version Control

This Policy should be reviewed annually, or at a minimum every 2 years by the Head of Legal and Governance who must also ensure the Policy requirements are well communicated to staff.

Any material amendments proposed to this Policy will need to be approved by the Board.

Non-material amendments (i.e., changes in role titles, formatting, etc.) may be made by the Head of Legal and Governance who has authority to make those non-material amendments.

Adopted by the NSFSL Board on 29 September 2019

Reviewed by the NSFSL Board on 22 June 2022.