3 November 2025

Practice Note: Declaring data breaches, data losses and cybersecurity attacks

Digital Identity Services Trust Framework (DISTF) Regulation 6(1)(d) requires an application for accreditation to include "information about any data breaches, data losses, or cybersecurity attacks previously experienced by the applicant, and any controls implemented following those events".

This requirement allows the Trust Framework Authority (TFA) to assess how an applicant manages information security risks and demonstrates maturity in responding to, mitigating, and learning from past incidents.

This practice note is intended to support applicants in determining whether information around data breaches, data losses or cybersecurity attacks should be disclosed to the TFA when applying for accreditation as a Trust Framework provider.

Definitions

Data breach: unauthorised or unintentional release, transmission or transfer of data.

Data loss: exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Cybersecurity attack: any event that jeopardises or may jeopardise the confidentiality, integrity, or availability of an information system or the information a system processes, stores, or communicates.

Disclosures

Applicants should take a pragmatic approach when identifying and describing past incidents. When deciding which incidents to disclose to the TFA, applicants should consider the severity, impact, and relevance of each incident.

Disclosure is expected when:

- The incident was critical or serious[1], and relates to the service(s) for which accreditation is sought; or
- The incident's potential impact was critical or serious and relates to the service(s) for which accreditation is sought; or

[1] As defined below

- The incident resulted in loss or breach of proprietary, sensitive, or classified information, particularly when it occurred within the last three years; or
- The incident jeopardised the confidentiality, integrity, or availability of an information system, particularly when it occurred within the last three years.

Security impacts

Applications should disclose previous incidents with a 'critical' or 'serious' impact or potential impact.

Levels	Description	Examples
Critical	Incident affecting critical systems or data, with potential to impact operations, revenue, customers, or result in information disclosure.	Distributed Denial of Service (DDoS) attack, unauthorised system access, multi-system ransomware.
Serious	Incident affecting noncritical systems or information, causing operational disruption or customer impact.	Malware on a single system, compromised credentials, minor unauthorised data access.
Low	Minor or potential incidents with limited operational or information impact.	Blocked phishing attempts, isolated employee security investigations.