SECURITY INCIDENT COMMUNICATION COMMITMENTS

How Clevermore Notifies Clients of Security Incidents

Clevermore serves law firms whose practice depends on the confidentiality of client information. When a security event affects, or has the potential to affect, our customers' data or service, our clients have a right to know — promptly, accurately, and through a channel they can rely on. This policy sets out the commitments we make to every Clevermore customer about how and when we communicate during a security incident.

All Clients Notified | Defined Timelines | Designated Contacts | Written Follow-Up

Our Commitment

If a confirmed security incident affects a Clevermore customer's data, environment, or service, Clevermore will notify that customer. Notifications are not opt-in, are not gated on contractual tier, and are issued whether the underlying cause sits inside Clevermore's systems, in a sub-processor, or in a shared piece of infrastructure we rely on.

Our default posture is over-disclosure rather than under-disclosure. If we are uncertain whether a particular customer is affected, we will notify and clarify, not stay silent and wait.

> **Scope.** This policy covers Clevermore's notification commitments to its customers. It is distinct from our internal incident-response runbook (which governs how we detect, contain, and remediate) and from any statutory breach-notification obligations to regulators or data subjects, which we comply with in parallel under applicable law (GDPR Art. 33, U.S. state breach-notification statutes, and contractual terms).

What We Treat as an Incident

For the purposes of this policy, a "security incident" is any confirmed event in one of the following categories:

- **Unauthorized access** to customer data, customer infrastructure, or production systems that store or process customer data.
- **Unauthorized disclosure** of customer data to a party not entitled to it, whether through misconfiguration, exfiltration, or accidental routing.
- **Unauthorized modification or destruction** of customer data, including ransomware events.
- **Loss of availability** of customer-facing services where the root cause is malicious activity (denial-of-service, credential abuse, infrastructure compromise).
- **Sub-processor or vendor incidents** that Clevermore has been notified of and that materially affect customer data we are responsible for.

Routine operational issues — transient outages, degraded performance, and bugs without a security component — are handled through normal support and status channels and are not covered by this policy.

Severity & Notification Timelines

Every confirmed incident is assigned a severity tier based on the sensitivity of the data involved, the scope of customers affected, and whether the event is ongoing. Tier determines how quickly we commit to issuing an initial notification.

TIER	DESCRIPTION	INITIAL NOTIFICATION
Critical	Confirmed exposure, exfiltration, or destruction of customer data; ongoing attacker access to production systems.	**Within 24 hours**
High	Confirmed unauthorized access to systems that store or process customer data, with no confirmed exposure of the data itself.	**Within 48 hours**
Medium	Sub-processor or upstream-vendor incident affecting infrastructure we use, with no confirmed exposure of Clevermore customer data.	**Within 72 hours**
Low	Security-relevant events that do not meet the bar above but that a reasonable client would expect to be informed of.	**In the next scheduled security update**

Notification windows are measured from the time Clevermore confirms an event meets the definition above — not from the time the event first occurred. We will continue to provide updates at a cadence appropriate to the severity until the incident is closed.

How We Notify

Notifications are delivered by direct email to the security and operational contacts each customer designates during onboarding. Customers are responsible for keeping these contacts current; we will accept updates at any time at security@clevermore.ai.

An initial notification will include, to the extent known at the time of writing:

- The nature of the incident and the systems involved.

- The categories and, where determinable, the volume of customer data affected.
- Whether the customer being notified is confirmed affected, potentially affected, or notified as a precaution.
- The actions Clevermore has taken to contain the incident and the actions we recommend the customer take.
- The cadence on which updates will follow and the named Clevermore contact responsible for those updates.

For Critical-tier incidents, we will additionally attempt direct phone contact with the customer's designated security lead.

Post-Incident Review

Within 30 calendar days of closing a Critical or High-tier incident, Clevermore will provide affected customers with a written post-incident summary. The summary will cover the root cause as best determined, the timeline of detection and response, the customer-facing impact, the remediation completed, and the longer-term changes Clevermore is making as a result.

Customer-specific facts are kept out of summaries shared with other customers. Where a regulatory or contractual obligation requires more detail than the summary contains, that detail is provided on request.

Regulatory & Contractual Alignment

This policy is designed to operate alongside Clevermore's broader compliance posture — including GDPR Article 33 notification obligations, U.S. state breach-notification statutes, and customer-specific data processing addenda. Where a contract or statute requires a shorter window or additional content, the stricter requirement controls.

Contact

Security-related communication of any kind — including updates to designated contacts, questions about this policy, and reports of suspected incidents — should be sent to **security@clevermore.ai**.