CHILDREN'S INTEREST CONTINUUM™
SECURITY INCIDENT & BREACH RESPONSE POLICY

Effective Date: July 14, 2026

---

1. Purpose

Children's Interest Continuum™ ("CIC," "we," "us," or "our") is committed to protecting the confidentiality, integrity, and availability of information processed through the CIC Platform ("Platform").

This Security Incident & Breach Response Policy describes CIC's approach to identifying, evaluating, responding to, and communicating security incidents involving Platform systems or user information.

---

2. Scope

This Policy applies to security events involving:

- Platform infrastructure;
- user accounts;
- stored information;
- authentication systems;
- Platform services;
- authorized third-party service providers.

This Policy applies to information processed through the Platform, including where applicable:

- account information;
- case information;
- evidence;
- uploaded materials;
- communications;
- other User Data.

---

3. Security Incident Definition

A security incident is an event that may affect the confidentiality, integrity, or availability of Platform systems or information.

Examples may include:

- unauthorized access;
- suspected account compromise;
- improper disclosure;
- malicious activity;
- security vulnerabilities;
- service disruption affecting data protection.

Not every security event constitutes a legally defined data breach.

CIC evaluates incidents based on applicable circumstances and requirements.

---

4. Incident Response Principles

CIC's response approach is guided by the following principles:

Identification

CIC works to identify potential security concerns through:

- operational monitoring;
- user reports;
- system alerts;
- security reviews;
- service provider notifications.

Assessment

CIC evaluates reported or detected incidents to determine:

- what occurred;
- what information may be involved;
- potential impact;
- appropriate response actions.

Containment and Remediation

Where appropriate, CIC may take steps to:

- limit unauthorized access;
- secure affected systems;
- address vulnerabilities;
- restore normal operations;
- prevent recurrence.

Communication

Where required or appropriate, CIC communicates relevant information regarding confirmed incidents.

---

5. Protection of User Information

CIC maintains security practices designed to protect User Data, including:

- secured storage systems;
- access controls;
- authentication requirements;
- case-based permissions;
- operational safeguards.

CIC does not sell User Data or intentionally disclose confidential information except as permitted by applicable agreements or law.

---

6. Incident Evaluation

When a potential incident is identified, CIC evaluates relevant factors, including:

- nature of the event;
- information involved;
- affected users;
- likelihood of harm;
- applicable legal obligations;
- contractual requirements.

---

7. User Notification

If CIC determines that notification is required under applicable law or contractual obligations, CIC will provide appropriate notice.

Notifications may include:

- description of the incident;
- categories of information involved;
- recommended user actions;
- steps CIC has taken or plans to take.

Notification timing and content may vary depending on:

- legal requirements;
- investigation status;
- security considerations.

---

8. Professional and Attorney Users

Professional users remain responsible for their own obligations regarding:

- client confidentiality;
- professional conduct requirements;
- client communications;
- regulatory responsibilities.

CIC's incident response process does not replace a professional user's independent obligations.

---

9. User Responsibilities

Users should assist in maintaining security by:

- protecting account credentials;
- reporting suspected unauthorized access;
- reviewing case permissions;
- removing unnecessary collaborators;
- maintaining secure devices and accounts.

Users should promptly notify CIC of suspected security concerns.

---

10. Third-Party Service Providers

CIC may rely on trusted service providers necessary to operate Platform functionality.

Where applicable, CIC evaluates and manages service provider relationships consistent with operational and security needs.

Security incidents involving service providers may be addressed according to applicable agreements and response procedures.

---

11. Security Reporting

Users who believe they have identified a security issue should report it through CIC's designated support or security contact channel.

Reports should include:

- description of the concern;
- relevant details;
- steps to reproduce, if applicable;
- contact information for follow-up.

Users should not attempt unauthorized access, testing, or exploitation of suspected vulnerabilities.

---

12. Updates to This Policy

CIC may update this Security Incident & Breach Response Policy as security practices, Platform functionality, or legal requirements evolve.

Updated versions will include a revised effective date.

Contact Information

Children's Interest Continuum™

629-204-4820

End of Security Incident & Breach Response Policy