Communities Connected for Kids Information Security Risk Assessment and Risk Management Procedure

Memo for Policy CCKids 1119

A documented and maintained Enterprise Information Security Risk Assessment is a HIPAA requirement and represents the basis of Communities Connected for Kids' Information Security Management Program. The risk assessment process allows for the identification and categorization of risks, determination of risk treatment methods, and development of procedures for ongoing monitoring and review of implemented safeguards.

Risk Assessment Review Process

The following represents the procedural elements of the Enterprise Information Security Risk Assessment as referenced in Communities Connected for Kids Policy 1119 Risk Assessment and Risk Management Policy.

1. **Technical Review**. Technical input is supplied by the CCKids IT through ongoing communications among staff, within project work groups, and at Devereux Lan Admin meetings. Communities Connected for Kids IT also leads reviews of new risks and areas of potential exposure fo Communities Connected for Kids, based on the following:
    a. Any new systems or processes in place or being considered (i.e., infrastructure changes, new applications, etc.).
    b. Vulnerabilities reported in the technical community.
    c. New technologies and methodologies Communities Connected for Kids users may be adopting.
    d. Findings from any externally conducted evaluations (penetration tests, social engineering audits, etc.).
    e. Evidence of particular styles of attacks (e.g., ransomware and CEO fraud emails).

2. **Operational Review**. Operational input is supplied by the Communities Connected for Kids IT Staff and Communities Connected for Kids Senior Management Team. Reported security and privacy incidents and discussions at Communities Connected for Kids Senior Management Team meetings provide context on the risks observed at the center level, encompassing categories such as user behavior, endpoint security, proper use, records management, and physical security. That information will be incorporated into the risk register and considered as new initiatives are evaluated.

3. **Assess Risk**. Based on the technical and operational input, the risk register of the Enterprise Information Security Risk Assessment is updated. See section below on *Risk Assessment Evaluation Criteria* for a description of how this is completed. New risks are entered at the bottom of the form and ratings applied based on controls in place, if any, at the present. For existing risks, if a new control has been put into place or there has otherwise been something about that risk that requires updating, the impact, likelihood and other ratings would be adjusted to reflect current status.

4. **IT Security Roadmap.** The Risk Management Plan takes the form of an IT Security Roadmap, a living document that registers risk mitigation activities.
   The Roadmap is organized by security program component and includes reference to the Risk Assessment Control Objective numbers so it is clear which risks are being mitigated

by any given section and to offer a direct tieback to the Enterprise Information Security Risk Assessment.

DocuSigned by:

Approval: Carol Deloach
96C0E7A7E02E4BA...

Date: 7/27/2022

Carol Deloach, CEO