ECNO/OASBO Vetting of Applications for Security and Privacy (VASP) Project – Call for Secondment

ECNO is seeking to fill a position through secondment arrangements with school boards or through employment contracts to support the day-to-day operations of the VASP Project. The position will begin as soon as possible and will be for a one-year term (until August 31, 2024) with the option to extend additional 1-year terms subject to funding. The commencement date for this position is open to negotiation with the ECNO office.

Preference will be given to bilingual (French / English) candidates.

We are seeking a 0.5 FTE Security Analyst position.

Security Analyst Role:

- Background in school Board Information Technology along with experience in data and network security.

Please see attached job posting/description and share with members at your board.

If you are interested in this position, please provide a covering letter and detailed resume and Email to Wayne Toms, ECNO Executive Director at ed@ecnoconnect.org no later than Friday, October 13, 2023 at 4:00 pm.

Thank you,
Wayne Toms
Executive Director
ECNO
ed@ecnoconnect.org
Phone: (519) 568-7899
Mobile: (705) 872-8910

Privacy Analyst

Position Summary:
Under the direction of the Executive Director (ED) and the Project Steering Committee, the Privacy Analyst's role is to perform Application Vetting for Privacy and Security.

Responsibilities:

- Using the evaluation tool developed by the PIM/ICT working group to consider if data of a personal nature is collected within the working environment of the application. If no personal information is collected or retained by the application, the title examination ends.
- The process is an in-depth electronic test that examines not only what the vendor describes as a user experience but pushes these boundaries to determine how robust internal barriers are. The technology team examines what a user can do and not necessarily what they are supposed to do. Typically, depending on the type of application being vetted, the team will adopt the positions of what can I do as an educator; as a parent; and as a student. Instances where access is given to information that ought to be secured, each of these breaches are documented as areas of concern and catalogued as issues to be followed up with for vendors. Once the electronic evaluation is complete, the evaluation begins with the team focusing on scoring each element based on the results of the electronic testing, information in the Privacy Policy and information contained in the Terms and Conditions. Scoring options for each question are offered to provide the greatest flexibility in achieving a fair outcome for all. An overall security rubric is contained within the examination structure in order that the team can provide their professional opinions about the kinds of information collected and it purported safety and use.
- Each evaluation yields information and mitigating strategies for adopters of the application to be aware of. These strategies are provided in common sense language and are the guidelines that educators, parents, and students should follow to limit the risk of their personal information becoming public.
- At the end of this process, an evaluation document containing the raw scores, mitigating strategies, questions for vendors, and overall assessment comments is compiled and uploaded to the data repository by the team.

Job Requirements:

- Excellent level of oral and written communication
- Excellent relationship skills
- Demonstrated commitment and self-discipline required to work in a virtual "work at home" environment.
- Excellent planning, organizing, decision making and problem solving skills
- Experience in school Board Data Privacy and familiarity with related legislation, i.e. MFIPPA,

Security Analyst

Position Summary:

Under the direction of the ECNO Director of Business Development (DBD) and the Project Steering Committee, the Security Analyst's role is to perform Application Vetting for Privacy and Security.

Responsibilities:

- Using the evaluation tool developed by the PIM/ICT working group to consider if data of a personal nature is collected within the working environment of the application. If no personal information is collected or retained by the application, the title examination ends.
- The process is an in-depth electronic test that examines not only what the vendor describes as a user experience but pushes these boundaries to determine how robust internal barriers are. The technology team examines what a user can do and not necessarily what they are supposed to do. Typically, depending on the type of application being vetted, the team will adopt the positions of what can I do as an educator; as a parent; and as a student. Instances where access is given to information that ought to be secured, each of these breaches are documented as areas of concern and catalogued as issues to be followed up with for vendors. Once the electronic evaluation is complete, the evaluation begins with the team focusing on scoring each element based on the results of the electronic testing, information in the Privacy Policy and information contained in the Terms and Conditions. Scoring options for each question are offered to provide the greatest flexibility in achieving a fair outcome for all. An overall security rubric is contained within the examination structure in order that the team can provide their professional opinions about the kinds of information collected and it purported safety and use.
- Each evaluation yields information and mitigating strategies for adopters of the application to be aware of. These strategies are provided in common sense language and are the guidelines that educators, parents, and students should follow to limit the risk of their personal information becoming public.
- At the end of this process, an evaluation document containing the raw scores, mitigating strategies, questions for vendors, and overall assessment comments is compiled and uploaded to the data repository by the team.

Job Requirements:

- Excellent level of oral and written communication
- Excellent relationship skills
- Demonstrated commitment and self-discipline required to work in a virtual "work at home" environment.
- Excellent planning, organizing, decision making and problem solving skills
- Experience in school Board Data Security and a background in school Board Information Technology.