UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment ("PIA")

PIA # 20-017 (Privacy Officer to Assign) ManageEngine ADAudit Plus

Form A

Please review the entire form before you answer any questions. Providing more information than the questions asks, providing information answering the wrong questions, or leaving sections blank will delay Privacy Officer approval.

In the following questions, answer the open ended questions in the **bolded** prompts. Keep bold font on all answers provided. Answer **Yes / No** questions by deleting the answer that does not apply. Do not add open ended text to **Yes / No** responses.

Name of Department: **GIS Lab**
PIA Drafter: **Matt McLean**
Email: **matt.mclean@unbc.ca** Phone: **250-960-XXXX**
Oversight Provided by: **Ian Hartley**
Email: **Ian.Hartley@unbc.ca** Phone: **250-960-6054**

Description and Scope of Information Management

Describe the purpose of your project/initiative/software. Describe a brief high level overview of the functions, who will benefit from those functions, and who will be impacted if that is not transparent. Indicate if there are groups that are restricted from use and the reason for proposed restrictions. Describe whether there are other reference documents including previous PIAs, whitepapers, or compliance documentation that may support this assessment.

ADAudit Plus records what individual accesses what files, when and how (Open, Modify, change permissions, Delete etc) by identifying them through their Microsoft Active Directory information. ADAudit Plus is intended to mitigate security vulnerabilities by identifying when individuals are granting read-write permissions to inappropriate individuals on our file servers. In real-time, ADAudit Plus ensures critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with up to 200+ detailed event specific GUI reports and email alerts.

All Elements of Information or Data

Using concise point form, please list the elements of information or data involved in the initiative, even if no personal information is involved. This could include client's name, age, address, work/home email, work/home phone number, educational history, employment history, work status, health information, financial information, photos, comments on a blog, or information specific to your subject area.

Active Directory Information (i.e. username) and activity on systems (access management details, metadata demonstrating any changes, and file names)

Location of Where Information is Managed

Does the information manager, vendor, and / or service provider operate from an office outside of Canada? **Yes**

Does any user of the information managed in this initiative access this information from outside of Canada beyond during short-term temporary travel? **No**

Does this initiative have any components that temporarily process information outside of Canada? **No**

Does this initiative store information for operational use outside of Canada? **No**

Does this initiative back up or make additional or redundant copies of information outside of Canada? **No**

Privacy Officer Comments, Conditions & Concerns

This PIA is based on a review of the material provided to the Information Governance Officer as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA update and submit for approval.

This appears to be a strictly on-premise managed auditing system which draws information from existing systems within UNBC and manages it in the GIS lab where ADAudit Plus is stored. Any changes to the location of the data system will require a Privacy Impact Assessment amendment. The PIA drafter has contacted the Chief Information Security Officer to ensure that ADAudit Plus does not cause any security vulnerabilities.

The use of auditing software is compliant with section 26(c) for collecting information to meet an operational requirement to ensure that the servers housing UNBC information are secure, 26(e) for collecting information to evaluate how well UNBC meets its security requirements and section 30 for ensuring that institutional data is protected from invasive disclosure and breach. Information will only be used for purposes consistent with the purposes of collection. Data produced from these audits will only be disclosed internally as required under section 33.1(1)(e) to the supervising Dean, staff under the Chief Information Security Officers' supervision, and the audited individual unless that information needs to be disclosed further to Human Resources and law enforcement to prevent or mitigate criminal behavior, or must be surrendered by court order.