UNIVERSITY OF ALBERTA

PRIVACY AND SECURITY ON-LINE TRAINING AND ACKNOWLEDGEMENT

QUESTIONS AND ANSWERS FOR EMPLOYEES

Do Faculty members have to do the on-line training and acknowledgement?

Yes, Faculty members are University employees who handle personal information in the course of their employment, including student information. They also generally access University information technology resources. Faculty participation is important to the success of this initiative.

Do sessional instructors have to do the on-line training and acknowledgement?

If a sessional instructor is a University employee and accesses either personal information in the course of their employment (e.g. student information), or accesses University information technology resources, then he/she is required to do the training and acknowledgement.

Do contractors have to do the on-line training and acknowledgement?

This initiative is focused on University employees, and there is no general requirement for contractors to do the on-line training and acknowledgement at this time. However, some units may wish to have their contractors complete the training and acknowledgement. Any contractor with a CCID can access and complete the training and acknowledgement.

Alternatively, a contractor may be provided with a hard copy of the training and acknowledgement, or the unit may organize a session for contractors to view and listen to the on-line training with a University employee, using the employee's CCID to access it.

Do I have to do the training and acknowledgement in one sitting?

No, you can complete the acknowledgement and different portions of the training at different times, if this is easier than completing everything in one sitting.

Is this initiative imposing a lot of new responsibilities on me?

No - it's important to remember that you already have an obligation to comply with privacy legislation and with the University's existing security and privacy policies and procedures. This new initiative is meant to help you understand what those obligations are, and how to fulfill them.

What if I don't feel comfortable signing the Acknowledgement because I still have questions about what I should be doing after I take the training and look at the policies and procedures?

Please ask any questions that you have! Questions can be directed to your supervisor, your unit's FOIP Liaison Officer, the Information and Privacy Office or the Chief Information Security Officer (contact information is set out below).

How will compliance be monitored?

- Each employee's completion of the training and the acknowledgement will be recorded electronically.
- Reports about the completion status of individuals within a Department ID will be generated and provided monthly to the designated contacts for this initiative within a Faculty or unit.

- Deans, Chairs, Directors and other supervisors are responsible for ensuring that the employees who report to them complete this process.

What are the consequences if I don't comply?

- Please remember that, regardless of whether or not you complete the training and "click" the Acknowledgement, all employees of the U of A are bound by the University's policies and procedures. Non-compliance with those policies and procedures constitutes misconduct and may be pursued under the applicable collective agreements, University policy, or law. We are educating you through this process so that you will know how to comply.

- Remember also that if you refuse to comply with the direction to take these steps and in future you cause a privacy or security breach (intentionally or unintentionally), your refusal to go through this education process may be a factor that is considered in the University's response to the incident.

I'm a researcher. If I accidentally lose a research participant's information or get hacked, isn't that really just my problem to deal with? Why should I have to do this?

- Apart from the impact on the research participants, if you have a privacy or security breach involving your research data, it doesn't just impact your reputation; it can impact the reputation of other researchers at the University, and the University as a whole.

- The Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans states that researchers shall safeguard information entrusted to them, and institutions shall support their researchers in maintaining promises of confidentiality. The on-line training and acknowledgement are one of the ways in which both you and the University fulfill these responsibilities.

- The recent discovery by the National Research Council of malware installed by hackers on its computers illustrates that hackers are interested in research information. We're implementing this initiative to help you make sure that you stay one step ahead of them.

Contact Information

Questions About How To Complete The Process

Information Services and Technology

(780) 492-9400
helpdesk@ualberta.ca

Questions About the Initiative As a Whole

Information and Privacy Office

Director, Information and Privacy - Diane Alguire
(780) 492-2252
diane.alguire@ualberta.ca

Office of the Vice-Provost & Associate Vice-President (Information Services & Technology)

Chief Information Security Officer - Gordie Mah
(780) 492-8607
gordie.mah@ualberta.ca