

Boilerplate Security Contacts disclosure

Draft - Boiler plate to send to Security Contacts twice a year

If you are receiving this email it means that you are subscribed to the Sakai security announcements list. The contact list is maintained by the Sakai Security Working Group (aka Security WG). To report any issues, please email security@apereo.org and your request will be forwarded to the Security Working Group.

We invite you to review your own status and that of subscribers from your institution to ensure that all contacts who need to be notified are subscribed to the list. Only authorized individuals are permitted on this list. Please see our Security Policy - <https://confluence.sakaiproject.org/display/SECWG/Security+Policy>

The security contacts list provides the Sakai Community with a private notification channel for issuing security alerts and patches ahead of any public disclosure. Designated security contacts are also provided access rights to view, comment and address issues flagged as security items in Sakai's JIRA issue tracking application.

Why is it important to pay attention to this information and follow the guidelines?

The integrity and security of existing Sakai installations can be compromised by the premature public disclosure of security threats. As an enterprise system, we have an obligation to behave responsibly and minimize the risks to institutions using the software. As a community, we have a responsibility to each other, our students, our faculty, our researchers and administrators to provide as safe an environment as possible.

What to do if you are notified of a security issue through this list?

Read the security notice carefully
Check the relevant Jira's. The Jira ids will be provided. If you do not have access, contact sakai-security@apereo.org .
If you need additional clarification, post your question on the Jira in the Comments.
Apply the fixes as soon as possible.
Do not ask questions on the Jira or to the Security WG. Do not post questions or information on any other web site, forum, email group, social network, or any other public communications forum.

What to do if you find what you believe to be a security vulnerability in Sakai?

Please notify sakai-security@apereo.org immediately. Describe the issue in detail. There is no such thing as too much information. Please include your telephone number in case we deem it necessary to contact you other than by email. Please do not take any other action and refrain from voicing your concerns on any public listserv, blog or other communication channel. We will get back with you as soon as possible with any further information or instructions.

If you file a Jira issue

Please make sure to flag it as a security issue by selecting "Security Issue" from the security level drop down.

Thanks for your attention,
On behalf of the Sakai Security WG