Vulnerability Disclosure Policy

At Alumna we take security of our users' data very seriously. If you have discovered or believe you have discovered potential security vulnerabilities in the Alumna Service, we encourage you to disclose your discovery to us as quickly as possible in accordance with this Responsible Disclosure Program.

We will work with you to validate and respond to security vulnerabilities that you report to us. Public disclosure of a security vulnerability could put the entire Alumna community at risk, we require that you keep such potential vulnerabilities confidential until we are able to address them. We will not take legal action against you or suspend or terminate your access to any Alumna Services, provided that you discover and report security vulnerabilities in accordance with this Vulnerability Disclosure Program. Alumna reserves all of its legal rights in the event of any noncompliance.

Capitalized terms not defined in this Vulnerability Disclosure Program shall have the meaning set forth in our Terms and Conditions.

Discovering Security Vulnerabilities

We encourage responsible security research on the Alumna services and products. We allow you to conduct vulnerability research and testing on the Alumna Services to which you have authorized access. In no event shall your research and testing involve:

1. Accessing, or attempting to access, accounts or data that does not belong to you or your Authorized Users,
2. Any attempt to modify or destroy any data,
3. Executing, or attempting to execute, a denial of service attack,
4. Sending, or attempting to send, unsolicited or unauthorized email, spam or other forms of unsolicited messages,
5. Testing third party websites, applications or services that integrate with the Alumna Services,
6. Posting, transmitting, uploading, linking to, sending or storing malware, viruses or similar harmful software, or otherwise attempting to interrupt or degrade the Alumna services, and
7. Any activity that violates any applicable law.

Issues not to Report

The following is a partial list of issues that we ask for you not to report, unless you believe there is an actual vulnerability:

- Cross-site request forgery (CSTF) on forms that are available to anonymous users
- Disclosure of known public files or directories (e.g. robots.txt)
- Domain Name System Security Extensions (DNSSEC) configuration suggestions
- Banner disclosure on common/public services
- HTTP/HTTPS/SSL/TLS security header configuration suggestions
- Lack of Secure/HTTPOnly flags on non-sensitive cookies
- Logout Cross-Site Request Forgery (logout CSRF)
- Phishing or Social Engineering Techniques
- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Sender Policy Framework (SPF) configuration suggestions

Reporting Security Vulnerabilities

If you believe you have discovered a security vulnerability issue, please share the details with Alumna by contacting us on info@alumna.eu

Alumna will acknowledge receipt of your report within 2 business days, provide you with an estimated timetable for resolution of the vulnerability, notify you when the vulnerability is fixed.

Email communication between you and Alumna, including without limitation, emails you send to Alumna reporting a potential security vulnerability, should not contain any of your proprietary information. The contents of all email communication you send to Alumna shall be considered non-proprietary. Alumna, or any of its affiliates, may use such communication or material for any purpose whatsoever, including, but not limited to, reproduction, disclosure, transmission, publication, broadcast, and further posting. Further, Alumna and its affiliates are free to use any ideas, concepts, know-how, or techniques contained in any communication or material you send to Alumna for any purpose whatsoever, including, but not limited to, fixing, developing, manufacturing, and marketing products. By submitting any information, you are granting Alumna a perpetual, royalty-free and irrevocable right and license to use, reproduce, modify, adapt, publish, translate, distribute, transmit, publicly display, publicly perform, sublicense, create derivative works from, transfer and sell such information.