Version 3.0 Date 02/07/2025

1. What is responsible disclosure at Bocconi

At Bocconi University, we consider the security of our systems a top priority. Nevertheless, no matter how much effort we put into system security, vulnerabilities might still be present.

If you discover a vulnerability, we would like to know about it so we can take the needed steps to address it as quickly as possible.

2. What we expect from you

- You must e-mail your findings to soc@unibocconi.it
- Only the following domains are in scope *.unibocconi.it and *.sdabocconi.it
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading data or deleting or modifying other users' data. In other words, when you are investigating one of our systems, bear in mind the proportionality of the attack. We will always take your report seriously and investigate any suspicions of a vulnerability, even without proof.
- The principle of minimal intervention applies when investigating potential system weaknesses. Verification should be limited to the most essential evidence required to validate a technical finding. For example, if a database structure is discovered, demonstrating its organizational framework is sufficient, without exploring its specific contents.
- Mere technical capability does not imply permission. If a vulnerability reveals potential system weaknesses, limit any investigative interaction to the absolute minimum required for verifying the vulnerability's existence. If you encounter any data during testing (such as Personally Identifiable Information, Protected Health Information, credit card data, or other information), cease testing and submit a report immediately.
- Do not reveal the problem to others until it has been resolved.
- You will delete all confidential information and other data you obtained during your investigation. You must provide written confirmation of this deletion
- It is strictly forbidden to use techniques based on physical security, social engineering, distributed denial of service, brute forcing, spam, or third-party applications.
- Do provide the necessary steps to reproduce the vulnerability, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex ones may require further explanation.
- Adherence to the established reporting protocol demonstrates professional responsibility and ethical conduct in vulnerability disclosure.
- Make every effort to avoid privacy violations, degradation or interruption of services, and destruction of data. In this sense, it is expressly forbidden to:
    - Access, modify or download data from an account for which you do not have rights;
    - Implement actions like "Denial of Service" attacks or capable of damaging the operation of any asset or resource;
    - Upload, connect, execute, or send malicious code after exploiting a vulnerability you found; for example, if you find a way to execute arbitrary code on a system, you cannot use it to gain more access to the system

- Conduct tests whose effect is to send unwanted messages, spam or other forms of unauthorized messages;

3. Vulnerability examples

- The following is a non-exhaustive list of examples of out-of-scope vulnerabilities:
  - Results of automatic vulnerability assessment/penetration testing/Information Gathering tools (e.g. SQLmap, Owasp ZAP, nmap, etc.);
  - Other reports related to low-impact vulnerabilities, such as clickjacking, weak captchas, lack of flags on cookies (e.g. secure, HTTPOnly), lack of HTTP security headers. SPF, DKIM, DMARC issues.
  - TLS configuration weaknesses, for example weak cipher suite support or the presence of TLS 1.0 support.
- Examples of in-scope vulnerabilities:
  - Remote Code Execution (RCE)
  - SQL injection
  - XML External Entity Injection (XXE)
  - Authorization bypass/escalation
  - Sensitive information leaks
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - Underprotected API

4. What you can expect from us

If you conform to the above rules, we promise that:

- We will respond to your report within 3 business days with our evaluation of the report
- We will resolve the vulnerability as soon as possible (the amount of time required to fix a vulnerability depends on several factors, among which the severity and the complexity of the issue at hand)
- We will keep you informed about the progress towards resolving the problem
- We will handle your report with strict confidentiality, and won't disclose your personal details to third parties without your permission
- We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication of the problem after it is resolved, if necessary.
- If you find a vulnerability in third-party software that we use and a bug bounty program covers that vulnerability, we will not try to claim this bounty.
- If, for any reason, more than one organization is involved, the basic principle is that the vulnerabilities can only be published if all organizations agree to this fact.

5. Issues excluded from the programme

While we are committed to maintaining the security of our systems, we cannot guarantee or be held responsible for potential legal actions by third-party service providers or vendors in response to good-faith security research and vulnerability disclosure.

- We do not provide legal protection against potential claims from third-party service providers.
- We cannot prevent or control potential legal actions that may be initiated by external service providers or vendors in response to security research.