SimBiotic Software Data and Process Protection Policy

June 22, 2026

1. Introduction

To operate efficiently SimBiotic Software ® (SimBio) must collect and use information about the individuals and institutions with whom it works. These may include current, past, and prospective employees, current and prospective customers (students and educational institution personnel) as well as suppliers. SimBio's Data and Process Protection Policy focuses on the data stored within the SimBio Active Learning System® as it is the only place within SimBio where data from students is stored.

In addition to protecting the data, SimBio must also ensure access to that data on a continuous basis when customers are using SimBio Active Learning System® to avoid disruptions to the customer's operations.

SimBio is committed to ensuring information is responsibly managed. SimBio will make every effort to meet its obligations under this policy and will regularly review these procedures and update them, as necessary.

SimBio's data security policy balances four principles against the needs of operating our business and fulfilling the needs of our users:

1. Minimize the amount and value of user data we store

2. Minimize the chances that user data is leaked or lost

3. Minimize both routine and unexpected downtime in the system

4. Have procedures in place to detect, inform, and trace sources of any losses or leaks in user data

2. Overview

SimBio's data security starts by limiting the data that is stored. SimBio only stores the following personal information about users of SimBio Active Learning System®:

- Name
- Email address
- Phone (optional)
- Student ID (or student identifier provided by LMS)
- Password (stored indirectly as a hash – not stored when accessing system via an LMS)
- Data from student work within SimBio Active Learning System® (such as answers to multiple choice questions)

SimBio deletes data from student work on a regular basis. Data on student work is not retained longer than one year after the end of the class in which they conducted the work.

SimBio does not store credit card information or other high value information. Even in the event of a data breach, there would be nothing of high value to be found within SimBio Active Learning System®.

In addition to limiting the data stored, SimBio has a variety of industry standard policies, processes, and systems in place to reduce the possibility of data loss. SimBio also has plans for recovering from and reporting data loss. Finally, SimBio has processes for software development and use of third-party libraries to reduce risks of unexpected outages or of vulnerabilities to data loss. These policies and processes are detailed below.

3. People and policies

SimBio's data security policy applies to all employees, contractors, agents, and representatives as well as temporary staff working for or on behalf of SimBio. A Data Controller appointed by SimBio management has overall responsibility for compliance with the SimBio Data and Process Protection Policy.

The SimBio Data and Process Protection Policy stipulates that anyone processing information must comply with following principles of good practice. The principles require that information:

- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
- Shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed
- Shall be accurate and where necessary, kept up to date
- Shall not be kept for longer than is necessary for that purpose or those purposes
- Shall be kept secure i.e. protected by an appropriate degree of security
- Shall not be transferred to an agency other than SimBio unless that agency ensures an adequate level of data protection
- Shall not be shared with third parties for promotional or marketing purposes
- Shall only obtain mobile and messaging opt in and consent for SimBio use. Mobile and messaging opt in and consent are never shared with anyone for any purpose.

Among the policies in place to reduce the chance of data loss are:

- Direct access to user data is only given to SimBio employees
- All employees and contractors sign non-disclosure agreements
- All employees with access to user data receive periodic training on cybersecurity
- All new employees submit to a background check prior to final offer of employment
- Each person with access to user data has their own individual login for accessing that data

- Each employee receives the minimal set of access to SimBio's systems and user data which will allow them to perform their duties
- SimBio periodically reminds employees and enforces the use of good passwords (upper and lower case, numbers, symbols, and/or randomly generated), and stores all passwords securely in a password management application
- When an employee leaves the company, their accounts to access company information are promptly invalidated

4. Systems

The SimBio Active Learning System® is hosted on cloud-based servers from AWS, and developers use personal computers for all development operations. As with many companies, SimBio relies on AWS, who maintains the physical hardware, for first-line protection of the servers and for maintaining operating system updates. AWS is currently SOC2 certified, and you can access their public SOC3 certification report here.

Among the systems we have implemented to reduce the chance of data loss are:

- Maintaining sensitive systems behind a VPN where possible
- Using https or similar encryption for transferring data to and from users and between internal systems
- Not storing or processing credit card information – all credit card processing is done directly by our provider for that service
- Protecting all employee's individual work-computers with passwords and anti-virus software
- Scheduling regular off-site backups

5. Company Processes

SimBio has implemented several processes that aid in preventing data loss and limiting the risk of malfunctions that could lead to downtime, among them:

- Using simulated data on test and development systems, or when real user data is required - de-identifying that user data before putting it on test and development systems
- Conducting periodic external vulnerability scans
- Conducting periodic cybersecurity training for employees who have contact with user data or other sensitive information
- Conducting scheduled tests of restoration of our systems in the event of an attack or failure
- Maintaining procedures for vetting 3rd party technology both upon adoption and when changes are made (see below)
- Reviewing this data and process policy yearly to update procedures to better address the goals of the policy given any changes in the threat environment and/or SimBio's own software and business

6. Process for Inclusion of 3rd Party Technology

SimBio necessarily relies on 3rd party technologies to build its applications, including both open-source and proprietary libraries. SimBio implements the following strategies to vet these technologies to minimize risks that could affect user data or continuous operation of the system:

- Verify that the technology under consideration is currently being supported by its developers
- Verify that the technology is in wide use and has an active community that collectively subjects the technology to scrutiny
- Conduct a search for any discussion of outstanding security issues with the technology including whether those issues have or are being addressed

7. The customer's right to access their personal information

Any person whose details are held by SimBio is entitled to ask for a copy of all information held about them.

When a request is received it will be dealt with as soon as possible, and in no case with a delay longer than 30 calendar days.

When providing the information SimBio will also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

8. Breach of the policy

Non-compliance with the requirements of this policy by members of our staff could lead to serious action being taken by third parties against SimBio. Non-compliance by a member of our staff is therefore considered a disciplinary matter that, depending on the circumstances, could lead to dismissal.

9. Procedures for Notifying Interested Parties in the Event of a Data Incident

If there is a breach of SimBio's database security or any other incident involving user data stored by SimBio, SimBio will, within 5 business days:

- To the best of our ability, notify all users who were directly affected by the data incident
- Notify the appropriate personnel at any institutions to which those users were associated in their use of SimBio's software
- Notify the appropriate personnel of any third parties, such as publishers, whose customers may have been affected by SimBio's data incident