GenScript ProBio Data Security

White Paper

GenScript PROBIO

Contents

1. Introduction to ProBio

1.1 Business Introduction

1.1.1 ProBio – Biologics CDMO

ProBio is the biologics CDMO segment of GenScript Biotech, proactively providing end-to-end service from drug discovery to commercialization with proactive strategies, professional solutions and efficient processes in antibody drug and gene and cell therapy to accelerate drug development for customers. ProBio, a subsidiary of GenScript Biotech Corporation, offers end-to-end CDMO services from drug discovery to commercialization with proactive strategies, professional solutions and efficient processes in CGT, antibody and recombinant protein drug, aiming to accelerate drug development for customers. ProBio has established companies in the United States, the Netherlands, South Korea, and China(Hong Kong, Shanghai, Nanjing and Zhenjiang) and other regions to serve global customers, and has helped customers in the United States, Europe, Asia Pacific and other regions obtain more than 90 IND approvals since October 2017.

ProBio's innovative solutions for antibody drug development include antibody drug discovery (hybridoma, antibody library, fully human transgenic mice, bispecific antibodies technologies, single b cell screening technology), antibody engineering (antibody humanization, affinity maturation, Fc Engineering) and antibody characterization (analytics and bioassays). In terms of biologics development service, ProBio has built a regulatory- compliant platform, from stable cell line development, host cell license, process development, analytical development to clinical manufacturing services, providing fed-batch and perfusion process to accelerate IND process and high quality material for clinical trials. ProBio has successfully delivered multiple CMC and GMP manufacturing projects. ProBio's total CGT solution covers CMC of plasmid, viral vector, mRNA vaccine and nucleic acid drugs for IND filing as well as clinical manufacturing and commercial manufacturing. ProBio integrated CMC solution for plasmid and viral vector including cell banking, process development, characterization and validation, analytical method development and validation, and stability study to enable cell and gene therapy go to next milestone.

ProBio's innovative solutions for biologics discovery and development include therapeutic antibody discovery, antibody engineering and in vitro/ in vivo pharmacology studies. In the biologics CDMO service, ProBio has built a DNA to GMP material platform, including stable cell line development, host cell commercial license, process development, analytical development to clinical and commercial manufacturing, and offer fed-batch and perfusion processes to meet the growing needs for antibody and protein drugs. ProBio has established GMP capacity that meets regulatory requirements of the US Food and Drug Administration (FDA),European Medicines Agency (EMA) and National Medical Products Administration(NMPA).

Toward the mission of "Innovation through Collaboration", ProBio is committed to helping customers shorten the timeline for the development of biological drugs from discovery to commercialization, significantly lowering R&D costs and shaping a healthier future.

For more information, please visit ProBio's official website https://www.genscriptprobio.com/

1.1.2 GenScript Biotech Corporation

GenScript Biotech Corporation (HK.1548) is an important technology and service provider in the world for life science R&D and manufacture. Built upon its solid DNA synthesis technology, GenScript Biotech comprises four major business units: a life science services and products business unit, a biologics contract development and manufacturing organization (CDMO) business unit, an industrial synthetic products business unit, and an integrated global cell therapy company.

GenScript Biotech was founded in New Jersey, USA in 2002 and listed on the Hong Kong Stock Exchange in 2015. The company's business operations span over 100 countries and regions worldwide with legal entities located in the U.S., China, Japan, Singapore, Netherlands, Ireland, the United Kingdom, Korea, Belgium and Spain. GenScript Biotech provides premium, convenient and reliable services and products for over 200,000 customers.

As of December 31, 2023, GenScript Biotech had more than 6,900 employees globally, and 87,700 peer-reviewed journal articles worldwide had cited GenScript Biotech’s services and products. In addition, GenScript Biotech owns a number of intellectual property rights, including over 300 patents, over 900 patent applications and great numbers of know-how secrets.

Driven by the corporate mission of “make people and nature healthier through biotechnology”, GenScript Biotech strives to become the most trustworthy biotech company in the world.

For more information, please visit GenScript Biotech's official website https://www.genscript.com

1.2 ProBio's Compliance Certification

ProBio adheres to international security standards and industry requirements by utilizing independent, third-party security services. These certifications encompass data security protection, oversight, governance, and assurance policies integrated throughout all business processes. ProBio collaborates with expert, independent third-party security, consulting, and auditing firms to assess its data security compliance from an unbiased perspective.

1.2.1 ISO 9001

ISO 9001 is a set of internationally recognized standards for quality management an internationally recognized standard for quality management and assurance issued by the International Organization for Standardization (ISO). Provide antibody drug and protein drug molecule discovery, pharmacology and pharmacodynamics research services, preclinical pharmaceutical development services for antibody drugs and protein drugs; Provide pre-clinical pharmaceutical study and clinical sample manufacturing services; Provide contract development and manufacturing services of plasmid for gene and cell therapy; Provide contract development and manufacturing services of virus for

gene and cell therapy; Provide contract development and manufacturing services of mRNA for gene and cell therapy, preventive vaccines; have all passed ISO 9001 certification. This denotes inspections of ProBio's management standardization and facilitates ProBio's sustainable, stable, and healthy development. ProBio will strictly implement the quality management system and various relevant rules and regulations, carry out production operations in strict accordance with standards, continuously improve product quality, and better provide customers with high-quality products and services.

1.2.2 ISO 27001

ISO 27001 is a strict set of information security management system standards widely recognized by the industry and is considered the global gold standard. ProBio and all other companies of GenScript Biotech Corporation share one integrated IT system, which is developed, maintained and supported by IT Department of GenScript Biotech Corporation. GenScript's IT department is ISO 27001 certified, and has always been regarded as the most authoritative and strict information security system certification standard in the world. ISO 27001 provides the best practice guidance for various organizations to establish and operate information security management systems. GenScript IT Department has passed ISO 27001. This means that ProBio has already been in line with international standards in the field of information security management, and has sufficient information security risk identification and control capabilities. That is, ProBio can provide secure and reliable services for customers around the world.

2. Data Security Protection Design

2.1 Data Security Protection Objectives

ProBio has designed a comprehensive and reliable defense system for data security, which can effectively protect data throughout the life cycle.

- **Lawful data gathering.** Using big data sorting technology, enterprises can lawfully collect sensitive data while adhering to legal boundaries.
- **Controlled access.** Access levels are defined based on the sensitivity of the data. Precautionary measures are implemented prior to data development and utilization to thwart unlawful exploitation.
- **Static data detection.** Through scanning and analysis, static data stored within systems is identified, and its distribution is presented comprehensively.
- **Real-time data monitoring.** Dynamic data is monitored to prevent unauthorized leakage during interaction and sharing.

2.2 ProBio's Methodology for Data Security System Development

In the development of ProBio's data security governance system, there are five key stages involved: business sorting, data classification and grading, strategy formulation, technology management and control, and strategy optimization. Data security governance encompasses the supervision and protection of data throughout its entire lifecycle, from policy implementation to practical application.

ProBio has devised a comprehensive and scientifically sound approach to data security governance, consisting of five main components: definition, detection, control, supervision, and practice.

- **Definition:** This involves analyzing company and industry policies, establishing norms for data usage among employees, and clearly defining sensitive data.
- **Identification:** Based on its sensitivity, data is positioned, classified, and categorized into different levels.
- **Control:** The available scope of data throughout its lifecycle is determined based on its sensitivity level and use policies and management platform to carry out fine-grained authority control on data.
- **Supervision:** Data is continuously monitored to ensure it is being used appropriately. Any unauthorized data access is recorded, providing clear evidence for subsequent investigations.
- **Practice:** ProBio tracks changes in data and provides services for operation and strategy optimization.

By integrating these data security governance methods into our business operations, ProBio can monitor data risks in real-time, visualize data usage, mitigate risk factors, issue timely warnings, prevent illegal data usage, and maintain continuous data security operations. This approach ensures ongoing monitoring and security of data.

2.3 Multi-Geo Data Security

ProBio has established global data storage centers, storing customer data in data centers in the US, Singapore or mainland China, depending on the compliance requirements of the country and region where the customer is located and the customer's choice. We also encrypt and store important categories of corporate and user data according to data classification to improve the security of important data. Data is backed up incrementally on a daily basis, fully backed up on a weekly basis, and recovery tests are conducted on a regular basis to ensure the security of data.

	China IT Team			**US IT Team**		
Data Center	Application Development	Application Deployment & Commissioning	Low-level Environment Commissioning	Application Development	Application Deployment & Commissioning	Low-level Environment Commissioning
China data center	√	√	√	×	×	×
US data center	√	×	×	×	√	√
Singapore data center	√	×	×	×	√	√

3. GenScript Group Data Security Support Organization

3.1 Risk Management and ESG Committee

GenScript Group has established an Risk Management and ESG Committee to adapt to the global strategic layout, manage various risks, internal control systems, and ESG strategies in the business process, and efficiently support the needs of business development. The committee's main duties include:

- Reviewing the Group's risk management policies and standards, internal control system and environmental, social and governance ("ESG") policies and guidelines, as well as the basic concepts and scope of compliance management;
- Supervise, guide and take the lead in organizing the implementation of risk management work;
- Regularly review risks and match key risks to strategic plans;
- Continuously identify, analyze, evaluate, monitor and report risks;
- Plan and implement risk management measures to control risks.

3.2 Information Security Committee

GenScript Group has established an Information Security Committee that is tasked primarily with analyzing and making decisions on significant issues related to information security, as well as reviewing and endorsing GenScript Group's relevant policies, objectives, work plans, and documents. Furthermore, the committee ensures the allocation of necessary resources for the orderly conduct of information security tasks and the effective operation of the information security management system.

The Information Security Committee functions as the core entity responsible for information security within GenScript Group. Its key duties include:

- Developing and executing an information security work plan.
- Overseeing, guiding, and coordinating the information security efforts of various departments and organizations.
- Establishing and refining GenScript's information security management system to ensure its ongoing effectiveness and continuity.

3.3 Data Compliance Committee

GenScript Group has established the Data Compliance Committee to ensure adherence to laws, regulations, and industry standards related to data management. The committee's main duties include:

- Defining the objectives of data compliance.
- Organizing and executing data compliance activities, including risk assessments.

- Monitoring changes in laws, regulations, policies, and business requirements, and regularly evaluating and enhancing data compliance management practices.
- Developing and reviewing relevant rules and regulations and overseeing their implementation.

3.4 Biosafety Committee

GenScript Group has established the Biosafety Committee to coordinate biosafety matters, ensure business compliance, and uphold laboratory safety standards. The committee's main responsibilities include:

- Developing and reviewing policies and guidelines related to biosafety.
- Making decisions on significant biosafety issues.
- Supervising and guiding the subcommittee to meet biosafety management requirements. This entails:
  - Developing and implementing laboratory biosafety management policies.
  - Conducting biosafety risk assessments.
  - Planning and evaluating activities related to pathogenic microorganisms and human genetic data.
  - Managing the declaration process for research and utilization of human genetic data.
  - Regularly assessing business compliance with biosafety regulations.

3.5 Special Statement

Currently, as a pivotal subsidiary under the GenScript Group, ProBio is thoroughly engaged in all the aforementioned committees of the group. In compliance with the unified standards and requirements of the group, ProBio has established a robust information firewall to safeguard its own data security and ensure its sustainable and sound operation.

4. ProBio's Data Lifecycle Security Management

4.1 Data Collection

During the data collection and generation phase, ProBio adheres to national laws and regulations. We employ a rigorous data extraction and aggregation process and implement robust security measures for collecting and acquiring data, particularly business data. This approach guarantees compliance across all data types and ensures thorough classification and quality control of the collected data.

4.1.1 Data Classification and Grading Management

Classification and grading involves analyzing various aspects of a data set, such as its specific attributes, security requirements, and distribution. We've developed a comprehensive data asset classification list, identifying data assets according to specific policies and methods that define the responsibilities for maintaining data security. Using this classification, we thoroughly assess the potential damage to national security, public rights, customer privacy, and enterprise interests if the data is compromised. ProBio then assigns grades and implements appropriate security measures.

Classification	Definition	Example
Top Secret	Refers to extremely confidential information. Any unauthorized dissemination will cause extremely serious threats and damage to the company's continued operation.	Such as unannounced company performance, proprietary technical information, gene plasmids provided by customers and other physical assets with intellectual property rights;
Confidential	Refers to information that is restricted to specific groups of people. Unauthorized dissemination may threaten and damage the company's normal operations.	Such as organizational structure, order information, original experimental data, etc.;
Shared Internally	It refers to information that is released to all employees within the company and is not intended to be disclosed to the public.	Such as internal recruitment notices, company event notices, etc.;
Public	Refers to information that is not restricted and can be released to the outside world.	Such as the company's annual report, company promotional materials, etc. that are officially disclosed to the outside world.

4.1.2 Data Collection Security Management

ProBio manages its data in compliance with laws, administrative regulations, and agreements with users. We prioritize both data application requirements and data security protection, ensuring adherence to relevant statutes and rules. To achieve this, we've established several data security protection policies. These policies outline the

purpose, usage, methods, scope, collection sources, and channels of data collection, while also verifying the legality and legitimacy of the data.

4.2 Data Storage Security

ProBio securely manages data storage. media and containers. We enhance security measures for sensitive data, including implementing backup and recovery procedures for vital data.

4.2.1 Security Management of Storage Media

Data storage media, including physical objects like magnetic or hard disks, and virtual ones like containers or virtual disks, can also be used for temporary data transmission. To ensure data security and prevent leaks, ProBio sets clear security standards for the usage of storage media, such as:

- Classifying the storage media.
- Grading storage media and defining specific requirements for each grade regarding data storage.
- Defining media usage standards and establishing media application and user registration policies.
- Establishing criteria, such as authority and access, for data cleaning and purging.
- Specifying labeling requirements for storage media, such as expiration dates.
- Regularly reviewing media usage and conducting inspections to prevent data loss.

4.2.2 Logical Storage Security Management

ProBio's security standards for storage containers and architecture encompass various aspects including authentication, access control, log management, communication protocols, and malware. We have outlined logical storage guidelines, which include:

- Defining logical storage systems and devices, such as cloud storage objects, block storage, and distributed storage.
- Establishing rules for logical security configurations, covering authentication, access control, and requirements for configuration changes and releases.
- Implementing measures for logical multi-tenant isolation and authorization management.
- Enforcing security management rules and operating procedures for storage equipment, including standards, maintenance, and emergency protocols.
- Specifying requirements for storage system accounts and rights, log management, encryption management, version upgrades, and other relevant aspects.

4.2.3 Data Storage Encryption Management

To ensure the confidentiality and integrity of data in storage, ProBio uses encryption technologies to encrypt and store data, preventing security risks such as interception, forgery, and tampering of authorized data, and ensuring the security of data in storage. Targeted encryption protection is carried out based on different categories and levels of data, especially for sensitive business data such as personal information and important data. ProBio can guarantee the security of sensitive data, regardless of whether data is leaked internally or externally, intentionally or unintentionally.

According to the requirements of national laws and regulations, requirements of service data for confidentiality and integrity, and data classification and grading, data is encrypted and stored in the scenarios demanding encryption and storage, and data storage scenarios involving sensitive service data or with high requirements for confidentiality and integrity.

4.2.4 Data Backup and Recovery Management

Disasters can strike unexpectedly, causing data system failures. Without backups, retrieving lost data becomes impossible. To ensure continuous access to information, ProBio regularly backs up and recovers data, ensuring redundancy in data management.

4.3 Data Transmission Security

4.3.1 Data Transmission Encryption

ProBio uses encryption measures like Transport Layer Security (TLS) for data transmitted over networks and encryption tunnels in virtual private networks (VPNs). This prevents interception, forgery, and tampering of data in insecure networks.

4.3.2 Protection Against Leakage During Data Transmission

ProBio employs anti-leakage tools to safeguard data during transmission, ensuring its security, especially for unstructured data.

4.4 Data Processing Security

During data processing, ProBio protects sensitive data, particularly business-confidential information, from damage, loss, or interception using an environmental security mechanism. Additionally, we control data access using the principle of least privilege, and we desensitize data in specific scenarios to ensure its security during processing.

4.4.1 Data Analysis Security Management

By taking appropriate security control measures during data analysis, ProBio can prevent security risks of leakage of valuable information and confidential information during data processing. The action of restoring anonymous data can be used to identify specific customers or projects and then to obtain valuable business information or sensitive data. To prevent such an action, ProBio has developed data resource operation rules and implementation guidelines during data analysis, defined available data sources and the scope of authorized use of various analysis algorithms, and defined relevant data protection requirements.

4.4.2 Data Opening Security Management

ProBio has created a data opening management policy based on classification and grading. This policy involves reviewing data contents beforehand, periodic reviews during data opening, and taking emergency measures if adverse effects arise post-opening.

4.4.3 Data Sharing Security Management

Based on data classification and grading, ProBio has defined the sharing level and appropriate protection measures regarding business attributes of the data, and has defined types, data contents, data formats, and sharing scenarios and ranges. ProBio has established the audit process of data sharing, defined the purpose of sharing, and conducted regular audit.

4.4.4 Data Interface Security Management

ProBio has set up rules for data interface security development, which define design requirements.

4.4.5 Data Desensitization Management

ProBio employs desensitization tools to protect sensitive data during analysis, especially customer and project information. Unique identifiers like order numbers are desensitized to ensure specific customers and project details cannot be recovered or located.

- **Data Desensitization:** ProBio employs desensitization technologies for numerical and text data, offering methods like irreversible encryption, random number masking, and mask replacement. These technologies automatically scan and identify sensitive information, ensuring efficient, convenient, and accurate desensitization.
- **Desensitized Data Distribution:** ProBio designs various desensitization scenarios and offers multiple distribution modes, including real-time options like database to database, database to file, file to file, and file to database. Desensitized data can be uploaded in real-time to target databases or file servers, stored locally on

desensitization servers, and forwarded as needed.

- **Data Comparison and Verification:** Before and after desensitization, ProBio verifies data and compares differences between source and target databases in terms of structure, objects, table count, and volume. Security administrators can assess task completion and the suitability of desensitization schemes.

4.4.6 Data Transmission Encryption Management

ProBio employs transmission encryption devices to secure transmitted data, prevent tampering or disguising, maintain the integrity and confidentiality of called data, and authenticate and audit the identities of personnel who call the data.

4.4.7 Data Destruction Security Management

ProBio sets guidelines for securely disposing of stored data, including procedures and requirements for the application, approval, and destruction of data and storage media. This prevents security risks of leakage of data in storage media caused by the loss, interception, or unauthorized access of stored data.

ProBio has developed the approval process and management methods for data destruction, including data destruction, cloud data destruction, and media destruction. The details are as follows:

- Defining the scenarios in which data needs to be destroyed, keeping business and data security in mind.
- Establishing the approval mechanism for data destruction.
- Destroying the data in an irreversible way.
- Recording the data destruction process to meet security audit requirements.

5. Access Control Measures

5.1 Security Access Management

In compliance with laws, regulations, and ProBio's business needs, we've created a security access management process to: define information access controls, prevent unauthorized access, enhance remote work management, and guarantee the security of company information in remote settings.

5.1.1 Authentication and Login Account Classification

System accounts are categorized as user, administrator, emergency, system service, system default, or temporary.

- User account: allows operational access to users.
- Administrator account: allows administrators to adjust system parameters, manage user accounts, and reset passwords.
- Emergency account: used solely in crisis situations when regular accounts are unavailable; it's not for daily use.
- System service account: facilitates system connections and manages system services.
- System default account: automatically created during system or application installation.
- Temporary account: created for short-term or one-time tasks, with a validity period typically under 3 days; no changes to permissions are permitted.

5.1.2 Certification Standard

Authentication data includes information like passwords, dynamic passwords, and transaction authentication details such as Personal Identification Number (PIN) and Card Verification Value 2 (CVV2). ProBio employs password authentication or strong authentication for systems storing confidential or higher-level data, safeguarding information confidentiality, integrity, and availability. All authentication data, including passwords, PINs, and CVV2, is secured during storage and transmission through encryption to prevent unauthorized access or modification. High-risk systems like fund management or financial systems require strong authentication, such as two-factor or biometric authentication, for access.

If a user notices any account issues, they're prompted to change their password right away. If needed, the security team can step in to investigate. If it's a serious incident like an attack or security breach, such as account interception or a brute force attack, it must be reported to the information security manager representative.

5.1.3 Login Standard

ProBio's internal information system implements the following security measures for login:

- Prior to login, appropriate warnings or security suggestions are displayed.
- Displaying plaintext passwords by default is prohibited, and successful and failed login attempts are logged.
- Original login failure reasons are not disclosed; instead, generic messages like "account password does not match" or "login authentication failed" are shown.
- Login failure control measures are in place: after five consecutive failed attempts within a set time frame, the account or IP address is locked, preventing further login for a specified period.
- Session timeouts are configured; if the system remains idle for over 30 minutes, the connection is automatically terminated or the user is logged out. If idle timeout isn't configured, alternative measures like Windows screen savers are used.
- The maximum number of concurrent sessions on a single system is limited.
- The number of simultaneous sessions allowed for a single account is restricted.

5.1.4 Account Management

Accounts are crucial for accessing our information platform, and each business holds valuable data. To ensure data security, ProBio implements the following measures for account management.

5.1.5 Account Standard

- Owners are designated for all accounts.
- A real-name registration system ensures each account corresponds to a specific user, preventing multiple users from sharing the same account.
- Under special circumstances, if more than one person needs to share the same account, it must be approved by the information security manager representative. Usage records must be maintained for tracking and review.
- Account owners are responsible for secure usage of accounts and bear the consequences of violating company security regulations or causing harm to company interests or others due to improper account use or safeguarding.
- Accounts inactive for 90 consecutive days are disabled or restricted from login.

5.1.6 Account Management Strategy

- Accounts are created and permissions granted via specified procedures, which are approved by department leaders. The account administrator ensures only essential system permissions are assigned.
- User accounts and permissions are reviewed every six months by the business department or account administrator. Inappropriate access is corrected promptly. Reviews are for deleting accounts and permissions only, not for creating or adding them.
- Accounts are disabled on the day an employee leaves their position.

- Disabled or locked accounts can be restored or unlocked after the account administrator confirms the user's identity or the information security department approves automatic unlocking or password resetting.
- System service accounts are strictly for system-to-system communication or managing system services, not for other purposes like system management.
- Default system accounts must be disabled, locked, changed, or configured properly to prevent unauthorized use. Default passwords are changed immediately after system setup.
- Emergency accounts must be used under the supervision of two personnel so that neither individual knows the complete account password.
- Special permissions for privileged tools are granted only with approval from the information security department, following the principle of least privilege. Regular reviews of privileged accounts are conducted by the information security department.

5.1.7 Password Management

Passwords are critical for account security, so ProBio enforces strict controls:

- Passwords must be at least 8 characters long.
- They must include a mix of uppercase letters, lowercase letters, numbers, and symbols.
- The user account name cannot be part of the password.
- Enable account risk alert, once the account is detected to be at risk, it is mandatory to change the password, with the new password differing from the previous six.
- Employees are prohibited from recording passwords on computers or paper.
- Using the same password across different platforms is not allowed.
- Sending passwords in plaintext, like via fax, is prohibited.
- When passwords are transferred via email, they must be sent multiple times, and senders must confirm receipt through non-email channels.
- If an employee forgets their password, the administrator verifies their identity before issuing a temporary password or assisting with a reset.

5.2 Authorization Management

Data permissions are fundamental for controlling data access, changes, and deletion. Following the principle of least privilege, ProBio specifices the following data authorization management methods.

5.2.1 Authorization Principles

- Permissions are role-based, with each role granted permissions according to its function.

- Specific authorizations for each function are required, allowing separate permissions for actions like reading, writing, modifying, deleting, and executing information assets.
- Authorization requests are based on work requirements and approved by the department head and information owner or designated manager.
- Access authorization follows the principle of least privilege, granting each user only the permission necessary to perform their job.
- Duty separation requirements must be met in access authorization, and conflicting authorizations are not allowed.

5.2.2 Access Management

- All ProBio information systems must have access control, especially those storing confidential data.
- Access policies must clearly outline access control rules and permissions for each user or group.
- Accounts and permissions of users which are no longer applicable (e.g., due to changes or resignations) must be promptly deleted or disabled.

5.2.3 Network and Network Service Access Control Management

- Network and network services are managed to restrict user access to authorized networks only.
- Firewalls and VLANs are used to logically isolate network domains, allowing only authorized information exchange.
- Cross-border network access is strictly controlled.
- Firewall policies follow a "deny by default" principle, permitting only necessary information flow and blocking unauthorized IP addresses.
- External users access the internal network securely through methods like VPN encryption or remote desktop.
- Remote diagnosis and configuration interfaces for information processing facilities are strictly controlled, disabled by default, and enabled when needed.
- External visitors can access ProBio's visitor network but require authorization from the head of the IT Department's or the information security manager to access the office network.
- Regular reviews of network access control policies are conducted to prevent inappropriate access.

6. Physical Security

6.1 Physical Area Partitioning

ProBio organizes physical security zones with a focus on hierarchical management and classified control, following these rules:

- Priority to services: Ensuring services run smoothly and efficiently.
- Streamlined structure: We aim for simplicity in designing security zones.
- Classified protection: Each security zone contains similar information assets and follows comparable security levels, environments, and policies.
- Continuous improvement: Security measures in each zone are continually updated and refined based on real-world circumstances.

Following these rules, ProBio determines the Business Impact Level (BIL) based on the highest security level for information in each department. This is done using the classification method outlined in the Information Security Management Policy and the BIA method in ISO 22301 Business Continuity Management. ProBio also considers potential threats and risks comprehensively when partitioning security areas for each department. Factors taken into account include:

- Average asset value: Security levels are determined based on each department's average asset value. For high-security assets, sub-security areas may be designated within departments, managed with appropriate high-security measures. Refer to the Information Security Management Policy for security level classification.

    (a) Highest asset value: 5+ top secret documents

    (b) Higher asset value: 2 to 4 top secret documents

    (c) High asset value: 1 top secret document

    (d) Medium asset value: 5+ confidential documents, but no top secret documents

    (e) Low asset value: < 2 confidential documents

- Risk grading: Departments receive security grade protection measures based on their actual information risk grade and threat severity. Risks are categorized as highest, higher, high, medium, or low, determined by the Information Security Risk Assessment and Management Rules. Services must be halted immediately for risk disposal at the highest risk level.
- Standards: In addition to relevant laws, regulations, and ProBio policies, other high-level security measures may be implemented.

Following these principles, ProBio's physical areas are categorized into four security levels, with level 4 being the highest and level 1 the lowest.

Level	Rank Factors	Typical Area
Level 1	Asset value and risk level are both "low" and there are no regulatory requirements	Reception room, parking lot, canteen hall
Level 2	At least one of the asset value and risk ratings is "medium" but no "high" rating	General office areas (excluding computer rooms, archives, finance, HR, IR, purchasing, marketing, internal audit, IT, etc.) and handover areas for import and export departments.
Level 3	At least one of the asset value and risk level is "high" but not "extremely high". Regulations have certain requirements.	All production areas, employee dormitories Finance, HR, Purchasing, Marketing, Internal Audit, IT, etc. in office areas.
Level 4	At least one of the asset value and risk level is "extremely high", or there is a clear requirement in regulations	Key laboratories of R&D department, core server room, archive room, investor relations department's data room, fire monitoring room, fire pump room, power distribution room, and back kitchen of canteen, etc.

6.2 Physical Security Control

As a leading biotechnology company, ProBio prioritizes providing secure, stable, sustainable, and reliable services to all customers. In line with international standards and data center regulations, ProBio has established a comprehensive security management system covering policies and processes. Through strict supervision and audits, ProBio continuously improves the physical security of its service environments.

ProBio deploys appropriate security control measures at the entrance and boundaries of its physical environment to prevent unauthorized access. Security measures, including physical security, access control, and security management, are tailored to the levels of different security areas. Consistency in physical measures is maintained across areas of the same security level.

6.3 Physical Protection Measures

6.3.1 Environmental Security Control

ProBio follows these rules for environmental safety control:

- When selecting security area sites, we consider natural and human-made disasters like fire, flood, earthquake, and more. We adopt additional measures to protect these areas.
- Security area establishments meet national requirements and include adequate fire, water, moisture, and theft prevention measures.
- We ensure regional power supply availability to prevent disruptions to daily work.
- Regional fire safety management in security areas meets national standards and is inspected by local fire authorities.

Equipment and archive rooms use gas fire control systems.

- Equipment rooms have automatic temperature and humidity adjustment capabilities, and key areas are electromagnetically shielded.

6.3.2 Building Safety Standards

ProBio enforces strict safety standards for its physical buildings, outlined as follows:

- The core equipment room complies with Class B data center construction standards.
- The archive room adheres to the Code for Design of Archive Buildings and Guidelines for the Construction of Enterprise Digital Archive Rooms.
- R&D laboratories are built following the universal biosafety standards outlined by the Architectural and Technical Code for Biosafety Laboratories and other applicable laws.
- According to ISO 27001, reception areas for key departments (e.g., Investor Relations and Finance) are designated. Important assets are secured in locked filing cabinets, safes, or information systems.
- Cable design is standardized and appropriate, ensuring isolation between power and communication cables. Power cables with different voltages and frequencies are also isolated to prevent interference.

6.3.3 Monitoring Area

ProBio has established the following security management rules for equipment room monitoring:

- For security areas below level 3, monitoring devices are placed at entrances, exits, and key passages, with surveillance video stored for at least 30 days.
- Level 3 security areas require monitoring devices inside the area, with surveillance video stored for at least 30 days.
- Level 4 security areas must install a 360-degree panoramic monitoring system, with surveillance video stored for at least 90 days.

6.3.4 Access Control System

ProBio's access control policies for data centers, office buildings, and other venues are:

- Below level 4 security areas: Entrances and exits require door locks or electronic access control. Special personnel manage key access and control rights.
- Level 4 security areas: Access control and fingerprint identification systems are installed. Access records are retained for over 180 days.

6.3.5 Alarm System

ProBio's alarm system management standards are:

- Security areas below level 3 do not require alarm systems except for the infrared intrusion detection system at the factory boundary.
- Level 4 security areas must have an intrusion prevention alarm system to deter unauthorized entry.

6.4 Personnel Access Management

Access to ProBio's security area requires authorization for all personnel. Employees must wear ID cards, while external visitors must register and obtain authorization before entering. The south and east gate booths serve as visitor handover areas.

6.4.1 Visitor Management and Control

ProBio's visitor rules are:

- For security areas below level 3, visitors use visitor IDs, and employees use employee IDs. Visitors must be accompanied by employees.
- For security areas at level 3, visitors initiate requests through the "AM06-Visitor Reception Application Process" on the OA and must be accompanied by employees to enter.
- Only dedicated full-time employees can enter level 4 security areas. Other employees or special visitors must apply through their respective departments and be accompanied by dedicated management employees. Entry and exit, as well as tasks, must be registered and records kept for over 90 days.
- Cleaning and security personnel must wear uniforms and identification badges. For level 4 security areas, they must also be accompanied by employees who work within level 4.

6.4.2 Identity Authentication Management and Control

ProBio's identity authentication rules are as follows:

- Personnel in each security area must wear either an employee card or a visitor card. Employees are prohibited from lending their cards to others. In case of a lost employee card, employees must promptly contact the HR Department.
- Employees can use their cards to access security areas below level 3.
- To enter level 3 security areas, employees must have the appropriate permissions encoded on their employee cards.
- Access to level 4 security areas requires permissions encoded on both employee cards and fingerprints.

6.4.3 Access Management and Control

ProBio's personnel access rules are:

- No separate permissions are required for security areas below level 3.
- Permissions for security areas above level 3 are granted based on employees' actual job requirements.
- Upon leaving the company, employees should return their employee cards to the department assistant. The assistant will then give the card to the HR department, which will cancel all access rights associated with the card.

6.4.4 Requirements for Devices Entering and Leaving Security Areas

ProBio has established rules for device management and control due to the potential for data transmission:

- Moving information devices within security areas without permission is strictly prohibited. Approval from the IT Department must be obtained, with written consent from the department head responsible for the device.
- Individuals entering a security area to move or unload devices must obtain prior authorization according to visitor management requirements. They must be accompanied by employees throughout the process.

6.4.5 Personnel Inspection, Training, and Assessment

ProBio conducts regular preventive maintenance for information devices across security areas. Responsibilities for maintenance personnel and supervision of the process are clearly defined. Annually, comprehensive inspections are carried out in equipment and archive rooms, alongside personnel training and assessments. Specific practices include:

- Routine inspections for security areas at levels 1 and 2, and both routine inspections and quarterly audits for levels 3 and 4.
- Employees in security areas below level 3 receive information security incident training through notices and special sessions organized by the Information Security Department.
- Employees in security areas above level 3 participate in annual information security training and assessments organized by the Information Security Department. They also study and analyze international and domestic information security cases to mitigate future incidents.

7. Operational Security

7.1 Terminal Security

The enterprise's internal terminals handle a significant volume of sensitive data, posing challenges to data security management and control due to their complex and evolving environment. Additionally, diverse personnel roles, usage scenarios, and cross-system data flow introduce more threats to data security. To address these issues, ProBio has implemented management and technical measures to safeguard data availability and security.

7.1.1 Desktop Security Management

Desktop terminal computers must be managed, monitored, and audited. The system oversees file and internet access, program usage, port communication, network sharing, printing, and other activities. Additionally, it manages desktop functions like message notifications, remote operations, remote assistance, remote control, and traffic.

7.1.2 Desktop Security and Audit

- Desktop user, permissions, and password management
- Terminal computer port management
- Antivirus software management
- Audit of end user changes
- Audit and management of file access
- Audit and management of online behavior
- Program audit and management
- Audit and management of the instant messaging program
- Network port communication audit
- Network sharing audit and management
- Audit of terminal user screens
- Audit and management of printing

7.1.3 Desktop Management and O&M

- Process operation management
- Software and startup group management
- Running software automatically by remote management
- Desktop message notification management
- Remote computer management
- System setting management
- Network connection and traffic management
- Terminal performance statistics

7.1.4 Storage and Peripheral Management

Peripheral and interface management involves overseeing the use of various peripherals and interfaces on terminal computers. ProBio establishes rules to deactivate certain peripherals and interfaces to prevent unauthorized usage. Specifically:

- Storage devices are deactivated.
- Use of certified mobile storage devices is allowed, but use of universal mobile storage devices is prohibited.
- Read-only permissions are configured for mobile storage devices.
- Authentication is required for mobile storage devices.
- Peripherals and interfaces are deactivated.
- Online and offline policy management is implemented.

7.1.5 Security Access and Unauthorized Connections

ProBio's data security monitoring platform detects and manages employee behaviors that attempt unauthorized internet or network access. This prevents illegal access and potential security risks or data leaks. Key features include:

- Online host monitoring
- Host authorization and authentication
- Blocking unauthorized host networks
- IP-to-MAC binding management
- Monitoring unauthorized terminal connections
- Blocking unauthorized terminal connections

7.1.6 Patch Distribution Management

Patch distribution management involves detecting system vulnerabilities and distributing and installing patches on terminal computers to enhance their robustness. ProBio's internal security administrator can customize software distribution and manage software and patching for employee application systems. Key components include:

- Automatic analysis of terminal computer vulnerabilities
- Patch distribution
- Management of patch distribution policies
- Testing patch integrity and compatibility
- Patch management
- Traffic control

7.2 Network Security

7.2.1 Security Protection Devices

Security protection devices are essential components of enterprise security. ProBio has deployed appropriate security devices at network, host, application, and data levels to comprehensively protect internal information assets. Currently, ProBio's security device deployment and protection on the intranet include:

- Firewall
- Web Application Firewall
- Intrusion Prevention System
- Intrusion Detection System
- Internet Behavior Management System
- Secure Mail Gateway

7.3 Log Management

7.3.1 Log Level Classification

ProBio labels internal logs as Fatal, Error, Warn, Info, and Debug. Production environment logs must use Info or higher, excluding the Debug level. Logs are further classified into system, application, middleware, and database categories. For each type of log, ProBio defines and implements the following security management measures:

- System logs: Generated by the operating system (including the virtualization system) and database management system, they contain system login, events, and errors.
- Application logs: Generated by application software, they include user login, data operations, errors, warnings, service audits, program tracking, data operations, and access logs.
- Middleware logs: Generated by middleware, they contain data operations, errors, warnings, and cached data.
- Database logs: Generated by databases, they include file and table logs that are managed by database management parties.
- Unified log naming convention: All log types must have unified names such as pafa, spri, acc, and gc.

7.3.2 Log Access Policies

ProBio's log collection management rules are outlined as follows:

- Log operations, including collection, backup, and monitoring, are standard in the default installation environment. For non-standard installations, the development and O&M departments collaborate on a log management scheme before initial deployment.
- New access requests must clearly specify the host, access path, tag for integration with the log management platform, and user management permissions for subsequent administrators. Requests are evaluated for appropriateness, and new system connections to the log management platform must be initiated within two business days of system provisioning.

- The access management platform approver verifies the specifics of connected servers and log paths for correctness and compliance. Log management platform approvers handle communication, coordination, and track interconnection processes within one business day.
- During interconnection, modifications to original requirements are not allowed. Exceptions include correcting log format errors for assigned accounts. New requirements necessitate log updates within two business days. In cases of delay, the requester is notified via email in advance.

7.3.3 Log Permission Management

ProBio has established the following policies based on the logs collected from its internal platform, hosts, servers, and business systems:

- Only O&M personnel have permission to view and download log files from production environment hosts, and these logs must be accessed through the log management platform.
- Third parties requiring access to host logs must request an account with limited log viewing permissions.
- The log management platform assigns administrator accounts for each system. Other personnel needing log access must apply to the subsystem administrator, with each department managing administrator accounts accordingly.
- Requests to download production environment log files require a service request submission. Due to delays with ProBio's unified log management platform and other factors, requests for special event handling or problem analysis may not be met immediately. For operations on production hosts, an exception request for log access must be submitted. After approval, operations can proceed under O&M personnel supervision.
- Any issues encountered by log viewers during subsequent usage (e.g., log format errors, adding or removing log collection paths) must be reported to the management platform approver for resolution.

7.3.4 Log Audit Policies

ProBio's log security audit policies are:

- The log audit supervisor reviews logs using the log management platform, checking for unauthorized actions and monitoring exception log frequency and duration. Any unauthorized behavior triggers an alarm.
- The default audit tool is the log management platform. Additional log audit analysis tools are used when necessary to ensure compliance with relevant laws, regulations, and ProBio's information security requirements.

8. Business Continuity

ProBio ensures business continuity and reliability through robust information security measures. This includes established reporting, response, evaluation, and punishment mechanisms for security incidents. We analyze incident causes and impact, provide feedback on processing, and learn lessons for improvement. Our emergency management includes meeting requirements for information system guarantee and recovery. We've enhanced our organizational and management abilities, as well as emergency handling capabilities. To prevent risks and minimize damage, we've developed a comprehensive emergency plan system.

8.1 Emergency Event Classification

ProBio categorizes emergency events into different levels based on severity, impact, and response needs.

Level	Explain
Particularly serious safety incidents (Level I)	Key information systems or related equipment and facilities related to the company's core business are damaged, and it takes 5 hours or more to restore the system/equipment function, resulting in extremely unsmooth information exchange and intelligence transmission between departments and between individuals; The company's top-secret information is leaked, destroyed and cannot be recovered or restored; Negative news attracts great attention from government departments or regulatory agencies, leading to investigations, or attracts great attention from the public media, leading to calls for action, causing irreparable damage to the company's reputation. It has a particularly significant social impact and even damages the brand image.
Major safety incident (Level II)	The company's key information systems or related equipment and facilities are damaged, and it takes more than or equal to 3 hours and less than 5 hours to restore the system/equipment function. This causes the information exchange and intelligence transmission between departments and between individuals to be blocked; The company's confidential information is leaked or destroyed and cannot be recovered or restored; Negative news is widely circulated within the industry or reported by national media, causing significant damage to a company's reputation. produce significant social impact.
General security incident (Level III)	Critical information systems/equipment facilities are affected, and it will take more than or equal to 1 hour and less than 3 hours to restore system/equipment functions. Information exchange and intelligence transfer between departments and between individuals are hindered to some extent; Internal public information is leaked or destroyed and cannot be recovered or restored; There is basically no impact on the company's reputation or the reputational impact caused can be recovered within a short period of time.

minor incident (Level IV)	The impact on operations is slight, and the critical production system is not interrupted or the recovery time after the interruption is less than 1 hour. Information exchange and intelligence transfer between departments and between individuals are slightly hindered; Information has not been disclosed or destroyed; Does not affect corporate reputation.

8.2 Emergency Response Process

In order to quickly respond to various security incidents and restore business data availability, confidentiality, and integrity, ProBio has developed an emergency response process as follows.

8.2.1 Security Incident Discovery

Employees must immediately report any observed or suspected information security vulnerabilities to the information security department. After analysis and identification, the information security department passes it to relevant technicians for resolution and logs it in the Information Security Incident Journal. The ProBio Information Security Department tracks the resolution progress. Employees who discover incidents, faults, or vulnerabilities must not alter anything until the report receiver handles it. Unauthorized testing or attempts to confirm vulnerabilities are prohibited without Information Security Department permission, as it could potentially harm information systems and services.

8.2.2 Security Incident Report

ProBio mandates prompt reporting of any discovered or suspected incidents, faults, or vulnerabilities. The employee who discovers the incident should report it to their department's information security representative or via dedicated email to the information security department. The department conducts initial analysis, determines the incident's type and level, and alerts the relevant personnel for resolution. For level I or II incidents, The Information Security Department should promptly report to the Head of the Process IT Department, who will then report to the company's Risk Management Committee and relevant external agencies as needed.

8.2.3 Security Incident Response

The department involved in an information security incident, along with the information security department and relevant departments, promptly takes effective measures to address the incident based on its nature and impact on company operations. This aims to minimize losses from the incident. The information security department is responsible for the initial response, following these principles:

- Contact relevant institutions promptly.
- Collect and preserve valid evidence, especially concerning employee involvement.

- Conduct investigations with minimal impact on information security, seeking external expert support if needed.
- Prioritize protecting personnel safety, sensitive devices, important data, system integrity, and minimizing company losses during incident handling.

8.2.4 Information Collection and Investigation

Upon receiving the information security incident report, the information security department conducts thorough investigation by collecting relevant data. This investigation forms the basis for analyzing, evaluating, and devising response strategies for the incident. The investigation includes examining:

- Network logs (e.g., routers, switches)
- Security device logs (firewall, intrusion detection system, antivirus)
- Server and application system logs
- Monitoring system logs
- Running processes and services (especially those enabling remote access)
- Suspicious user accounts (particularly unauthorized ones)
- Unexpected hidden files
- Timing and detection method of initial signs of the incident
- Systems and users involved

8.2.5 Analysis and Evaluation

The ProBio information security department conducts a preliminary assessment of the incident based on collected information. They analyze the incident, determine its type, and evaluate its severity level. Incident classification may be adjusted as more detailed information becomes available during incident control and handling.

8.2.6 Summary of Information Security Incidents

The ProBio information security department compiles a summary of incident handling, detailing the incident's causes, experiences, and lessons learned from each stage of the process. They discuss follow-up actions, including incident notification and implementation of corrective measures. All incidents are documented in the Information Security Incident Journal, and the information security department generates an Investigation Summary Report based on records, experiences, evaluation results, and post-incident investigations. This report is required for incidents classified as level II or higher and prepared as necessary for lower-level incidents.

8.2.7 Reward and Punishment

ProBio enforces strict review and takes information security incidents seriously, with the following rules in place:

- Departments and individuals contributing to incident handling are rewarded to reduce incident occurrence, enhance handling efficiency, and ensure business continuity.
- Those not adhering to regulations, causing adverse events and losses, face punishment.
- Reward and punishment measures are determined by the Employee Reward & Penalty Policy, with severity of incidents, losses, and causes informing the extent of punishment.

8.3 Emergency Drill

To bolster its own business security management, ProBio refines its emergency response process for its business systems, aiming to minimize system downtime and ensure security. It conducts regular simulated emergency drills covering various security scenarios, including:

- DDoS attack prevention
- Hacker intrusion countermeasures
- Data recovery
- Disaster recovery procedures
- Data center catastrophes (such as fire or flooding)
- Data leaks
- Phishing
- Malware
- New vulnerability attacks

During these drills, employees swiftly identify, analyze, and address situations using ProBio's monitoring, management, and protection platforms, promptly reporting to the information security department. These drills enable ProBio to handle security incidents promptly, enhance security awareness among internal organizations, departments, and employees, establish robust security standards, and safeguard customer data.

9. External Audit

GenScript Group regularly hires third-party external audit firms to conduct audits of the group. The most recent audit was conducted in the fourth quarter of 2023, when BSI was hired to audit the group's information security management system and Deloitte was hired to audit the group's information security risk management. The audit results were good.

www.genscriptprobio.com

Email：infosec@genscriptprobio.com

GenScript PROBIO