2024

Data Protection and Storage Policy – CSBT Campus

CSBT CAMPUS | 859, Colombo Road, Kurana Negombo

Table of Contents

Data Protection and Storage Policy of CSBT Campus

1. Introduction.

CSBT (Cambridge School of Business and Technology) Campus recognizes the critical importance of protecting data and ensuring its integrity, confidentiality, and availability. This Data Protection and Storage Policy outlines the guidelines and procedures for handling data across the campus to maintain compliance with legal requirements, protect sensitive information, and mitigate risks associated with data breaches.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who handle, store, or have access to data within CSBT Campus premises or information systems.

3. Data Classification

CSBT Campus classifies data based on its sensitivity and criticality:

- Public Data: Information intended for public disclosure.

- Internal Data: Information for internal use only, not intended for public disclosure.

- Confidential Data: Sensitive information requiring heightened protection due to legal, regulatory, or proprietary reasons.

4. Data Handling and Storage and Disposal Guidelines

4.1. Access Control:

- Access to data should be granted on a need-to-know basis.

- User authentication mechanisms such as passwords, biometrics, or multi-factor authentication should be implemented.

- Regular reviews of user access privileges should be conducted to ensure appropriateness.

4.2. Encryption:

- All confidential data must be encrypted during transmission and storage.

4.3. Data Storage:

- Data storage devices (servers, databases, etc.) must be physically secured in access-controlled areas.

- Redundant backups should be maintained in geographically diverse locations to mitigate the risk of data loss.

- Regular audits of data storage infrastructure should be conducted to ensure compliance with security standards.

4.4 Data Disposal:

- When data is no longer needed, it should be securely erased from storage devices using industry-standard data wiping techniques.

- Physical media containing data must be destroyed using secure methods (e.g., shredding) before disposal.

5.0 Data Retention:

- Data should be retained only for the period necessary to fulfill its intended purpose or as required by Sri Lanka PERSONAL DATA PROTECTION ACT NO: 09 OF 2022

- Refer to data retention schedule below.

5.1. Student Records

- Admissions Records: 5 years after admission decision.
- Application Forms, Transcripts, and Recommendation Letters: 5 years after admission decision.
- Admission Denied Records: 2 years after decision.

5.1.1 Academic Records

- Transcripts: Permanent.
- Grade Reports: Permanent.
  Class Lists: 5 years after graduation or last date of attendance.

5.1.2 Financial Aid Records

- Applications and Supporting Documents: 7 years after end of award year.
- Disbursement Records: 7 years after end of award year.

5.1.3 Graduation Records

- Degree/Certificate Awarded: Permanent.
- Graduation Lists: Permanent.

5.2. Employee Records

- **Employment Records**
- Job Applications and Resumes: 3 years after hiring decision.
- Employee Contracts: 7 years after termination.
- Performance Evaluations: 5 years after termination.
- **Payroll Records**
- Pay Stubs and Payroll Registers: 7 years.
- Tax Documents: 7 years, in compliance with tax regulations.
- **Benefits Records**

  Health and Insurance Records: 7 years after termination.
- EPF / ETF and Retirement Records: Permanent.

5.3. Administrative Records

- Board Meeting Minutes: Permanent.
- Accreditation Records: Permanent.
- Institutional Reports (Annual Reports, Strategic Plans): Permanent.
- Legal and Compliance Records
- Contracts and Agreements: 7 years after expiration.
- Litigation Files: 10 years after case closure.

5.4. Financial Records

- General Ledger: Permanent.
- Financial Statements (Annual, Quarterly): Permanent.
- Accounts Payable/Receivable: 7 years.
- Expense Reports: 7 years.

5.5. Facilities Records

- Building Plans and Blueprints: Permanent.
- Maintenance Records: 5 years after disposal of asset.

- Lease Agreements: 7 years after expiration.

5.6. IT and Data Security

- System Logs: 6 months
- Security Logs: 1 year.
- Access Logs: 1 year.
- Backup Tapes: 1 year, subject to space and specific needs.
- Incident Reports: 3 years.

5.7. Miscellaneous

- Library Records
- Catalogue Records: Permanent.
- Borrowing Records: 3 years after item return.

5.8 Research Data

- Research Proposals and Grants: 7 years after completion.
- Research Data: As per sponsor requirements or 7 years after project completion if no specific requirements.

5.9. Student Life Records

- Counselling Records: 7 years after last contact.
- Disciplinary Records: 5 years after graduation or last date of attendance.

5.10. Marketing and Public Relations

- Promotional Materials: 5 years.
- Press Releases: Permanent.
- Event Records: 5 years.

5.11. Health and Safety Records

- Incident Reports: 5 years.
- Safety Training Records 5 years.
- Health Records (Non-Medical): 7 years after termination.

By aligning the data retention schedule with the Sri Lankan Personal Data Protection Act, No. 9 of 2022, Cambridge School of Business and Technology ensures compliance with local data protection requirements, safeguarding personal data while meeting institutional and legal obligations. Regular reviews and updates to the schedule will maintain ongoing compliance and adapt to any changes in the legal landscape.

6. Data Handling Procedures

6.1. Data Transfer:

- Secure channels (e.g., VPNs, encrypted connections) must be used for transferring sensitive data.

- Data transferred via physical media (e.g., USB drives) should be encrypted and accompanied by appropriate authorization.

- Below guidelines from the Ministry of Education Sri Lanka on Handling Student Records should be adhered to.

6.1.1. Data Collection and Purpose Limitation

Purpose Specification: Collect student data for specified, explicit, and legitimate educational purposes.

Consent: Ensure that consent is obtained from students or their guardians for the collection of personal data, where applicable.

Minimum Necessary Data: Collect only the data that is necessary for the intended purpose.

6.1.2. Data Accuracy and Integrity

Accuracy: Ensure that student data is accurate, up-to-date, and complete.

Verification: Periodically verify and update student records to maintain accuracy.

6.1.3. Data Storage and Security

Secure Storage: Store student records in a secure manner to prevent unauthorized access, loss, or damage. This includes both physical records and digital databases.

Access Controls: Implement strict access controls to ensure that only authorized personnel can access student records.

Encryption: Use encryption for digital records, particularly when transmitting data electronically.

7. **Disposal**: Securely dispose of student records that are no longer needed, ensuring that personal data cannot be reconstructed or retrieved. Use methods such as shredding for physical records and secure deletion for electronic records.

7.0 Access and Confidentiality

7.1 Confidentiality: Maintain the confidentiality of student records. Do not disclose personal data to unauthorized individuals or entities.

7.2 Parental/Student Access: Allow students and their guardians to access and review the student's records, ensuring they can request corrections if necessary.

7.3Third-Party Access: Limit third-party access to student records and require appropriate safeguards when sharing data.

8. Data Breach Response

8.1 Incident Response Plan: IT Security: Identifies and mitigates security vulnerabilities.

HR: Addresses any employee-related issues.

Customer Service: Handles customer inquiries and concerns

8.2 Notification: Employees should report suspected breaches immediately to the Executive Director on 0767 147 831/ IT Security 0704933797

9 Compliance and Training

9.1 Compliance Monitoring: Regularly audit and monitor data handling practices to ensure compliance with legal requirements and guidelines.

9.2 Training: Provide regular training for staff on data protection principles, legal requirements, and best practices for handling student records.

10. Security Incident Response

10.1. Reporting:

- Any suspected or confirmed security incidents involving data must be promptly reported to the designated authority: Executive Director /IT Security 0704933797.

- Incident reporting procedures should be communicated to all employees and contractors.

10.2. Investigation and Remediation:

- Upon discovery of a security incident, a thorough investigation should be conducted to assess the impact and identify the root cause.

- Remedial actions must be implemented promptly to mitigate further risk and prevent recurrence.

11 Compliance and Enforcement

11.1 Training and Awareness:

- All employees and contractors should receive regular training on data protection policies, procedures, and best practices.

- Awareness campaigns should be conducted to reinforce the importance of data security: responsibility-Tranzire Technologies

11.2 Compliance Monitoring:

- Regular audits and assessments should be performed to ensure compliance with this policy.

- Non-compliance with data protection policies may result in disciplinary action, including termination of employment or contract.

12. Policy Review

This Data Protection and Storage Policy will be reviewed annually to incorporate any changes in legal requirements, technology, or organizational practices. Amendments to the policy will be communicated to all relevant stakeholders.

9. Conclusion

CSBT Campus is committed to safeguarding the integrity, confidentiality, and availability of data through the implementation of robust data protection and storage measures outlined in this policy. Compliance with these guidelines is essential for maintaining trust with stakeholders and mitigating risks associated with data breaches.

Sharing of staff or student documents, information, or databases with external parties is strictly prohibited without prior approval from the Executive Director or Head of Academic Affairs. Any breaches of this policy will be subject to necessary legal action.

Policy Review Date

01.01.2025

End of policy