CELESTE BEAUTY ACADEMY, INC.
IT-105 CYBERSECURITY INCIDENT AND DATA BREACH RESPONSE

Policy ID	IT-105	**Version**	1.0
Board Approval Date (Version 1.0)	November 15, 2026	**Date of Last Review**	
Statutory / Regulatory References	N.C. Gen. Stat. § 75-65; FERPA, 20 U.S.C. § 1232g; 2 C.F.R. § 200.303, as applicable.		

Establish an organized process to identify, contain, investigate, report, recover from, and document cybersecurity incidents affecting CBA systems or information. Applies to staff, board members, contractors, and service providers.

I. REPORTABLE EVENTS

Report suspected phishing compromise, ransomware, malware, lost or stolen devices, unauthorized access, mistaken disclosures, suspicious vendor activity, and loss of student, personnel, financial, or recruitment data. A security incident is not automatically a legally reportable data breach.

II. IMMEDIATE REPORTING

Anyone who suspects an incident must promptly notify the designated security coordinator or Executive Director through an approved channel. Do not delete messages, alter logs, investigate independently, or publicly discuss the incident. If a school account may be compromised, use an alternate trusted communication channel.

III. RESPONSE TEAM AND ESCALATION

Management shall designate an incident lead and involve IT, the Executive Director, legal counsel, affected data owners, relevant vendors, and the Board Chair as appropriate. The Board receives timely material-risk updates without unnecessary exposure to sensitive incident details. Identify conflicts of interest and use independent oversight when needed.

IV. TRIAGE AND CONTAINMENT

Record discovery time, affected systems, data categories, potential student impact, and evidence sources. Prioritize student safety and critical operations. Isolate affected accounts/devices, revoke compromised sessions, reset credentials, and preserve relevant logs and evidence under IT guidance.

V. INVESTIGATION AND LEGAL ASSESSMENT

Determine what happened, which records were accessed or acquired, the number and location of affected individuals, and whether information was encrypted or otherwise protected. Consult counsel to assess FERPA, North Carolina identity-theft/breach-notification law, contractual duties, insurance conditions, and any federal or grant reporting obligations. Do not assume one deadline applies to every incident.

VI. NOTIFICATIONS AND EXTERNAL COORDINATION

Only authorized leadership, in consultation with counsel, may notify affected individuals, regulators, law enforcement, insurers, vendors, or the public. Provide legally required notices within applicable deadlines and in required formats. Coordinate with the North Carolina Department of Public Instruction when required by law, contract, or program guidance.

VII. RECOVERY AND VALIDATION

Restore from verified clean backups, patch exploited vulnerabilities, rotate credentials, test system integrity, and monitor for recurrence. Management must authorize return to normal operations and document residual risks.

VIII. DOCUMENTATION AND PRESERVATION

Maintain an incident file with timeline, decisions, evidence, impact assessment, notifications, expenses, remediation, and lessons learned. Preserve records under litigation holds and applicable retention schedules; restrict access to sensitive investigative materials.

IX. TABLETOP EXERCISES AND IMPROVEMENT

Conduct at least one incident-response tabletop exercise annually after operations begin, update contact lists and vendor escalation paths, and track corrective actions to closure. Review this policy annually and after any significant incident.

X. INCIDENT CONTACT

Initial escalation: Executive Director or designated security coordinator. Privacy contact: President@celestebeautyacademy.com. CBA shall maintain a separate internal incident-response contact roster rather than publishing sensitive escalation details.

Implementation and Approval

This draft establishes proposed requirements. CBA shall identify responsible personnel, verify current technology and vendor practices, and obtain legal review before adoption. Management shall develop supporting procedures, forms, and training as needed. Nothing in this policy supersedes applicable law or an approved records retention schedule.