ANNEX C

TO THE BISCAST WEBSITE AND DIGITAL SERVICES POLICY | POLICY NO. 2026-ICT-001
ADOPTED: ADCO RES. 14, S. 2026 | APPROVED BY THE BOARD OF TRUSTEES: BOT RES. 88, S. 2026

WEBSITE MODULE SHUTDOWN AND INCIDENT RESPONSE MATRIX

Authority, notification and restoration protocol for module-level and site-level incidents

C.1 OVERVIEW

This Annex implements Sections 6 and 9 of the Policy governing module shutdowns, maintenance windows and incident response. A matrix of authorization levels, response actions and restoration targets is provided below.

C.2 SHUTDOWN AND INCIDENT RESPONSE MATRIX

Level 1 - Scheduled Maintenance (database optimization, content refresh)

Authority - Module Administrator with online validation through the System Modules manager.

Public Notice - standardized aesthetic maintenance notice naming the module, the reason and the expected restoration window; raw technical messages are never displayed to the public.

Targets - announcement at least 24 hours ahead when possible; every action documented in the System Module Audit Trail.

Level 2 - Unplanned Module Degradation (failed integration, data error)

Authority - SuperAdmin or SCPRO may immediately place the affected module offline; concerned managers are notified through the admin panel.

Public Notice - immediate replacement of the affected module with the institutional maintenance notice; status logged with timestamp.

Targets - triage within 2 hours; interim mitigation (reverting to the last validated state) within 24 hours.

Level 3 - Full Site Shutdown or Security Incident (breach attempts, systemic failure)

Authority - SuperAdmin; the VPAA and the MIS / ICT Director are informed immediately; the College President is notified for prolonged outages.

Public Notice - site-wide maintenance notice with the institutional header; all inbound links are preserved to avoid broken references.

Targets - immediate containment; coordinate with the Data Protection Officer under Annex D if personal data is implicated; RA 10173 breach notification timelines are observed.

C.3 ACCOUNTABILITY AND LOGGING

Every shutdown, restoration and incident event is recorded in the module audit trail with the initiating account, timestamp and reason. Records support the post-incident review and the semestral compliance report under Annex A.