Policy on the Use of Advanced Digital Technologies, Including Artificial Intelligence (AI) and the Internet of Things (IoT), in Support of Decision-Making, Operational Efficiency, and Service Delivery Across University Administrative and Academic Business Processes (GD7)

Strategic Vision and Institutionalization

- **Policy Alignment:** BASC shall adopt and institutionalize the responsible, ethical, secure, and strategic use of advanced digital technologies in alignment with the digital transformation agenda and policy directions of the Commission on Higher Education (CHED) for State Universities and Colleges (SUCs).
- **Core Technologies:** Core technologies include Artificial Intelligence (AI), the Internet of Things (IoT), smart campus systems, data analytics, cloud computing, and related emerging technologies.
- **Primary Objectives:** These tools will be deployed to enhance governance, improve operational efficiency, and strengthen service delivery across academic and administrative business processes.
- **Strategic Role:** Smart campus implementation is recognized as a key strategy to achieve innovation-driven, technology-enabled, and future-ready higher education services consistent with national digital transformation initiatives.

The Smart Campus Framework

- **Framework Prioritization:** BASC shall prioritize the development and implementation of a Smart Campus Framework that integrates interconnected digital systems, intelligent infrastructure, and data-driven technologies.
- **Operational Pillars:** The framework will support efficient campus operations, sustainable resource management, improved learning environments, and responsive public service delivery.
- **Scope of Initiatives:** Smart campus initiatives may include, but are not limited to:
  - Smart classrooms and automated attendance systems
  - Intelligent energy and water management
  - Campus-wide connectivity and digital identification/access control systems
  - Smart security, surveillance, environmental monitoring, and disaster preparedness systems
- **Expected Outcomes:** These technologies shall improve institutional responsiveness, operational sustainability, transparency, accessibility, and stakeholder experience across all university services.

Advanced Integration and Modernization

- **Functional Areas:** AI- and IoT-enabled technologies shall be integrated into:
  - Academic management, research, and innovation
  - Student support services, records, and information management
  - Facilities and asset monitoring
  - Institutional planning and performance evaluation processes
- **Decision-Making & Quality:** Integration aims to support evidence-based decision-making and continuous quality improvement.

- **Institutional Commitment:** The deployment of these technologies shall contribute to the modernization of SUC operations, supporting the college commitment to digital governance, operational excellence, and globally competitive higher education.

Legal Compliance and Data Privacy

- **Regulatory Compliance:** All implementations must comply with existing national laws, government regulations, and applicable policies of CHED, the Department of Information and Communications Technology (DICT), the National Privacy Commission (NPC), and other relevant regulatory bodies.
- **Statutory Adherence:** Strict adherence is required toward the Data Privacy Act of 2012 and its Implementing Rules and Regulations.
- **Core Protections:** BASC shall guarantee the protection of personal information, cybersecurity, intellectual property rights, and ethical standards across all deployment phases and interconnected systems.

Governance, Safeguards, and Ethics

- **Ethical Execution:** AI, IoT, and smart campus technologies must be implemented with appropriate human oversight to promote transparency, accountability, inclusivity, academic integrity, environmental sustainability, and data security.
- **Risk Management:** The college shall establish appropriate safeguards, cybersecurity protocols, and risk management mechanisms.
- **Asset Protection:** These mechanisms are designed to protect institutional data, digital assets, and critical infrastructure from misuse, unauthorized access, cyber threats, and system vulnerabilities.

Capability Building and Sustainability

- **Human Capital Development:** To sustain digital initiatives, BASC shall provide capacity-building programs, digital literacy and AI competency training, and technical assistance.
- **Target Stakeholders:** Training and support will be continuously provided to faculty members, administrative personnel, researchers, and students.
- **Accountability:** Continuous monitoring and evaluation mechanisms shall be established to track initiative progress.
- **Innovation Culture:** BASC shall encourage innovation, interdisciplinary collaboration, and research on emerging technologies to support institutional effectiveness, sustainability, quality assurance, and the realization of a smart, resilient university ecosystem aligned with CHED's vision.

General Do's and Don'ts

Do's

All stakeholders using institutional digital technologies and smart campus systems shall:

- Use digital technologies responsibly, ethically, and professionally;
- Protect usernames, passwords, digital signatures, and authentication credentials;
- Comply with institutional ICT, cybersecurity, and data privacy policies;

- Report cybersecurity incidents, vulnerabilities, or unauthorized activities immediately;
- Respect intellectual property rights and copyright laws;
- Ensure accuracy, integrity, and confidentiality of institutional data;
- Participate in required digital literacy and cybersecurity training programs;
- Use AI systems only for legitimate academic, research, administrative, and operational purposes;
- Promote responsible and ethical use of AI-generated outputs; and
- Support sustainability, transparency, and innovation initiatives of the College.

Don'ts

All stakeholders are strictly prohibited from:

1. Accessing systems, databases, or networks without authorization;
2. Sharing passwords, accounts, digital signatures, or confidential credentials;
3. Using AI technologies for plagiarism, misinformation, fraud, academic dishonesty, or malicious activities;
4. Collecting, processing, or sharing personal data without lawful authority or consent;
5. Installing unauthorized software, applications, or devices within institutional systems;
6. Disabling or tampering with cybersecurity and monitoring mechanisms;
7. Using institutional technologies for illegal, unethical, or non-official purposes;
8. Circumventing access controls or security protocols;
9. Engaging in cyberbullying, harassment, or misuse of digital communication platforms; and
10. Damaging, disrupting, or compromising institutional digital infrastructure and smart campus systems.

References

1. Commission on Higher Education (CHED)
2. Department of Information and Communications Technology (DICT)
3. National Privacy Commission – Data Privacy Act of 2012
4. Implementing Rules and Regulations of the Data Privacy Act of 2012
5. ADB Law and Policy Reform – Data Privacy Act of 2012

Prepared by:

MA. MELANIE A. CRUZ, DIT
Director, Digital Transformation Office

Approve by:

JAMESON H. TAN, EdD, CESE
SUC President III