Data Protection Policy

This system is designed to comply with Spanish Organic Law 3/2018 (LOPDGDD), the General Data Protection Regulation (GDPR), and the specific requirements for higher education institutions under the Spanish Organic Law 2/2023 (LOSU).

The following policy details the formal mechanisms used to protect institutional and student data.

1. Legislative Framework

All data processing and digital storage at C3S Business School are conducted in accordance with:

- **Spanish Organic Law 3/2018 (LOPDGDD):** Regarding the protection of personal data and the guarantee of digital rights.
- **EU Regulation 2016/679 (GDPR):** Ensuring the privacy and security of personal data within the European Union.
- **Organic Law 2/2023 (LOSU):** Governing the digital security requirements for university-level centres in Spain.
- **Spanish Royal Decree 311/2022 (ENS):** Adhering to the National Security Framework for electronic administration.

2. Digital Storage Protocols

C3S employs a "Security by Design" approach to managing digital assets:

- **Encrypted Infrastructure:** All digital student records and academic data are stored on **encrypted servers**.
- **Access Control:** Access is strictly limited through Multi-Factor Authentication (MFA) and role-based permissions, ensuring only authorised personnel can retrieve sensitive information.
- **Redundancy and Backups:** Automated backups are maintained in accordance with **IT Disaster Recovery Protocols** to prevent data loss due to hardware failure or cyber-incidents.
- **Physical-Digital Synergy:** While moving towards a paperless environment, any printed documents containing sensitive data are secured in locked filing cabinets with restricted access, mirroring the security of the digital environment.

3. Data Transmission and Cybersecurity

To maintain the integrity of data as it moves between departments or to external partners, the following measures are enforced:

- **End-to-End Encryption:** Data transmissions are encrypted and documented to prevent interception.
- **Penetration Testing:** The School conducts regular system audits and penetration **testing** to identify vulnerabilities and bolster cyber-resilience against evolving threats.
- **Cyber-Risk Modelling:** The Risk and Compliance Subcommittee proactively models cyber-risk scenarios—such as IT infrastructure expansion—to implement advanced firewalls and incident response protocols.

4. Institutional Accountability

Digital security is governed through a formal oversight structure:

- **The Risk Register:** Cyber-threats are a standing item on the Institutional Risk **Register**. They are evaluated using a Risk Matrix that ranks the likelihood and impact of data breaches.
- **Responsible Officers:** Each high-level digital risk is assigned a Responsible Officer tasked with monitoring and executing a dedicated Mitigation Plan.
- **Staff Training:** All administrative and academic staff undergo mandatory **Cybersecurity Training** to recognise phishing attempts and maintain data hygiene.

5. Student and Staff Digital Rights

In accordance with Spanish legislation, C3S guarantees the following digital rights:

- **Right to Rectification and Erasure:** Individuals may request the correction or deletion of their personal data.
- **Data Portability:** Students have the right to receive their digital academic records in a structured, commonly used format.
- **Confidentiality:** C3S maintains a zero-tolerance policy for unauthorised data disclosure, handled through the Ethics and Compliance Committee.