

Enterprise Architecture Principles

1. Enterprise Architecture Principles

Enterprise Architecture Principles represent the fundamental guidance governing how Technological University Dublin manages information, applications, technology and digital services. The principles provide a framework for decision-making and should be applied consistently across initiatives, projects, procurement activities and operational services.

The principles are intended to guide decision-making rather than prescribe specific technical solutions. They help ensure that information system investments support the University's strategic objectives while managing risk, cost and complexity.

Use of Architecture Principles

The principles may be used to:

- Guide the planning, design and implementation of information systems and technology services.
- Support architecture assessments and governance reviews.
- Inform procurement, supplier selection and contract management activities.
- Provide evaluation criteria for technology solutions and service proposals.
- Support portfolio management and investment decision-making.
- Assist in the development of standards, policies and operating procedures.
- Assess existing systems and services for alignment with the Enterprise Architecture.
- Inform roadmap development and technology lifecycle planning.

Applicability to externally provided services

These principles apply to all University information systems, technology services and digital capabilities, regardless of whether they are developed, operated, hosted or supported internally or by an external provider. Relevant architecture requirements should be incorporated into procurement, contracting, assessment and supplier-management processes.

2. Business Principles

Business Principles provide the foundation for decision-making across the University and guide the planning, implementation, management and evolution of information systems and digital services. These principles ensure that technology investments support Technological University Dublin's strategic objectives while managing risk, improving efficiency and delivering value to the University community.

BP-1: Primacy of Principles

Statement

These Enterprise Architecture Principles apply to all University administrative functions, business processes, information systems and technology initiatives. They provide the foundation for consistent decision-making regarding information management and digital services across TU Dublin.

These principles are not intended to limit academic freedom in teaching or research but rather to guide the management and governance of administrative and institutional information systems.

Rationale

These principles provide guidance for the use, development and evolution of the University's information systems. Consistent application of the principles promotes strategic alignment, reduces risk, avoids unnecessary costs and supports effective governance.

Implications

- All significant information system initiatives should be assessed for alignment with these principles before commencement.
- Architecture decisions should be documented and retained as governance records.
- Where compliance with a principle is not possible, the exception should be documented, justified and approved through appropriate governance processes.
- Principles should be considered collectively rather than individually.
- Where principles conflict, the rationale for the chosen approach should be documented.

BP-2: Maximise Value to the University

Statement

Information system decisions must seek to maximise value to TU Dublin as a whole, while appropriately balancing cost, risk, service quality, sustainability and long-term institutional benefit.

Rationale

Decisions made from an enterprise-wide perspective typically provide greater long-term value than decisions made solely for the benefit of an individual unit or

function. The University's resources should be directed towards solutions that support strategic priorities and generate measurable benefit for the institution.

Implications

- Technology investments should consider total lifecycle costs, including acquisition, implementation, operation, support and retirement.
- Existing capabilities should be evaluated before procuring or developing new solutions.
- Commercial, cloud-based and shared-service options should be assessed where they provide appropriate value, security and operational benefit.
- Solutions should favour configuration over customisation where practical.
- Information system initiatives should align with the University's strategic roadmap and enterprise architecture direction.
- Local preferences may occasionally need to be balanced against enterprise-wide benefits.
- Information solutions must be procured in compliance with all University Procurement rules.

BP-3: Maintain Transparency in Information Systems Decision-Making Statement

Information system decision-making should be transparent, collaborative and informed by appropriate stakeholder participation across the University.

Rationale

Technology exists to support the University's academic, research and administrative objectives. Effective outcomes are achieved when business stakeholders, subject matter experts and technology professionals work together to define requirements, priorities and expected outcomes.

Implications

- Stakeholders should participate in decisions proportionate to their responsibilities and the impact of the decision.
- Governance decisions should be communicated appropriately to maintain transparency and shared understanding.
- Risks should be identified, assessed and managed jointly by business and technical stakeholders.
- Significant decisions should be supported by appropriate analysis, evidence and documented rationale.

- Cross-functional collaboration should be encouraged throughout the lifecycle of information system initiatives.

BP-4: Business Continuity – Plan for Continued Operations

Statement

University operations should be capable of continuing, at an agreed level, during and following disruption to information systems or supporting technology services.

Rationale

The University relies heavily on information systems to support teaching, learning, research and administration. Appropriate planning for continuity and recovery minimises disruption and supports organisational resilience.

Implications

- Information systems should be assessed for criticality and business impact.
- Recovery requirements should be defined and proportionate to the importance of the service.
- Recoverability, maintainability and resilience should be considered during solution design.
- Backup, recovery and continuity arrangements should be periodically reviewed and tested.
- Operational risks should be actively managed through activities such as patching, vulnerability management and assurance reviews.
- Alternative operating arrangements should be considered where business continuity requirements justify them.

BP-5: Minimise Duplication – Common Use Applications

Statement

Information systems should be designed and selected to support University-wide use wherever practical, rather than creating multiple solutions that perform substantially the same function.

Rationale

Duplication increases cost, complexity, support effort and the risk of inconsistent business processes or conflicting information. Shared capabilities enable greater efficiency, consistency and value from technology investments.

Implications

- Existing enterprise capabilities should be assessed before new solutions are acquired or developed.
- Similar functionality should not be implemented multiple times without a documented justification.
- Where gaps exist in enterprise solutions, efforts should be made to address deficiencies rather than introduce duplicate systems.
- Shared services and common platforms should be preferred where they meet business requirements.
- Data supporting University decision-making should be standardised wherever practical.

BP-6: Maintain Legal and Regulatory Compliance

Statement

Information systems, processes and services must comply with all applicable legal, regulatory, contractual and University policy requirements.

Rationale

Compliance supports the University's legal obligations, protects institutional reputation and helps maintain the trust of students, staff, researchers, partners and regulators.

Implications

- Compliance requirements should be identified during planning, procurement and implementation activities.
- Information systems should support compliance with applicable laws, regulations and contractual obligations.
- Personnel should understand their responsibilities regarding compliance requirements.
- Existing non-compliant systems should be assessed and remediated where appropriate.
- Changes in legal or regulatory obligations may require changes to business processes, controls or technology solutions.

BP-7: Risk-Based Approach to Information Security

Statement

Information and information systems must be protected through a risk-based approach that maintains appropriate levels of confidentiality, integrity and availability.

Rationale

Risk assessment enables the University to identify threats, understand potential impacts and implement controls that are proportionate to the value of information assets and the risks they face.

Implications

- Information systems, data and technologies must be protected from unauthorised access, disclosure, alteration or destruction.
- Security controls should be proportionate to the sensitivity, value and criticality of information assets.
- Risk assessments should consider threats, vulnerabilities, existing controls, likelihood and potential impact and should be conducted on all applicable systems and services.
- Risk treatment decisions should be documented and reviewed.
- Security responsibilities should be clearly defined throughout the lifecycle of systems and services.
- Information security should be considered from project initiation through to system decommissioning.

BP-8: ICT Responsibility

Statement

Technology Services is responsible for the provision, operation and management of enterprise technology services, infrastructure and standards in partnership with business stakeholders.

Rationale

Successful delivery of information systems requires clear accountability, shared understanding of priorities and alignment between business needs, technology capabilities, service levels, security, risk and cost.

Implications

- Governance processes should support the prioritisation and delivery of information system initiatives.

- Business and technology stakeholders should jointly define requirements, priorities and expected outcomes.
- Service expectations, responsibilities and delivery commitments should be clearly understood.
- University defined information security, governance and compliance requirements are applicable to all information systems and services used by the university.
- Business process, data, application and technology architectures should be maintained to support decision-making and planning.
- Technology Services should provide standards, expertise and guidance to support alignment with enterprise architecture principles.

BP-9: Continuous Improvement

Statement

Information systems, technology services and associated processes should be continually reviewed and improved to maintain their effectiveness, efficiency and relevance.

Rationale

The University's operating environment, regulatory obligations and technology landscape continue to evolve. Continuous improvement enables TU Dublin to respond effectively to changing requirements and increasing expectations.

Implications

- Performance measures should be established and monitored to support service improvement.
- Industry standards and benchmarks should be used where appropriate.
- Opportunities for automation should be considered where benefits outweigh costs and risks.
- Service disruptions, incidents and problems should be analysed to identify improvement opportunities.
- Standard architectures, processes and practices should be reviewed periodically and updated as needed.
- Lessons learned from projects, audits and operational activities should inform future improvements.

3. Data Principles

Data Principles provide guidance for the creation, management, sharing, protection and use of university information assets. Effective management of data enables informed decision-making, efficient service delivery and compliance with legal, regulatory and operational requirements.

DP-1: Data is an Asset

Statement

Data is a valuable University asset that must be managed throughout its lifecycle to support teaching, learning, research, administration and decision-making.

Rationale

Data has value beyond the systems in which it is created and stored. Managing data as an asset enables the University to improve decision-making, enhance service delivery, reduce duplication and maximise the value derived from information resources.

Implications

- Data ownership, management and governance responsibilities should be clearly defined.
- Data should be managed consistently throughout its lifecycle, including creation, use, retention, archiving and disposal.
- Appropriate controls should be applied according to the value, sensitivity and criticality of the data.
- Information system initiatives should consider the impact on existing information assets.
- Data management activities should support both operational and strategic decision-making.

DP-2: Data is a Shared Resource

Statement

Data should be securely shared and made accessible to authorised users where required to support legitimate University activities, while respecting security, privacy and regulatory obligations.

Rationale

Appropriate access to reliable information supports collaboration, informed decision-making and efficient service delivery. Controlled sharing also reduces unnecessary duplication and repeated collection of information.

Implications

- Data should be captured once and reused where required in line with regulatory requirements.
- Information should be available to authorised users through approved mechanisms only.
- Data sharing should be based on business need and appropriate access controls.
- Technical and organisational barriers to appropriate information sharing should be minimised where practical.
- Information systems should support secure and controlled data sharing.
- Access should be based on legitimate business need, data sensitivity and least-privilege principles.
- Access to data does not automatically confer authority to alter, disclose or reuse it for another purpose.

DP-3: Common Vocabulary and Data Definitions

Statement

Data should be defined using common business terminology and consistent data definitions across the University.

Rationale

Consistent understanding of information improves communication, reporting, integration and decision-making. Common definitions reduce ambiguity and improve confidence in institutional information.

Implications

- Common business definitions should be established and maintained.
- Authoritative definitions should be used consistently across systems and reports.
- Information systems should support standard data structures wherever practical.
- Metadata and data definitions should be documented and maintained.

- Data standards should be governed through appropriate University procedures.

DP-4: Data Quality

Statement

Each data element shall have an accountable owner responsible for ensuring the quality, accuracy and integrity of that data.

Rationale

One of the primary benefits of an enterprise information environment is the ability to share information across organisational boundaries. As reliance upon shared data increases, confidence in the quality, consistency and integrity of information becomes essential. Authoritative sources and clear accountability help minimise duplication, inconsistency and errors.

Implications

- Data Trustees are accountable for the quality and integrity of the information under their responsibility.
- Users should have confidence that information is accurate, complete and fit for purpose.
- Information should be captured electronically and validated as close to the point of creation as practical.
- Appropriate data quality controls should be implemented for critical information assets.
- Data quality issues should be identified, monitored and addressed through established governance processes.

DP-5: Data is Easily Accessible

Statement

Authorised users must be able to access the information required to perform their duties efficiently and effectively.

Rationale

Timely access to information improves decision-making, service delivery and operational efficiency. Information should be accessible to those with a legitimate need while maintaining appropriate security and privacy controls through the application of least privilege principles.

Implications

- Information should be accessible through approved, secure and user-friendly mechanisms.
- Barriers to appropriate access should be minimised where practical.
- Access rights should be based on business need and the principle of least privilege.
- Information should be presented in a manner that supports usability and decision-making.
- Accessibility requirements should be considered when designing information services.

DP-6: Data Protection

Statement

Data managed by the University must be protected through appropriate measures that preserve its confidentiality, integrity and availability.

Rationale

The principles of data sharing and data accessibility must be balanced against the obligation to protect personal, sensitive, confidential and proprietary information. Data protection requirements must be considered throughout the lifecycle of information systems and services.

Implications

- Privacy and data protection considerations must be incorporated from the earliest stages of solution design.
- Privacy by Design and Privacy by Default principles should be applied to projects involving data.
- Data hosting and processing activities should be recorded for all information systems.
- Data Protection Impact Assessments must be completed where required.
- Information should be classified according to its sensitivity and protected appropriately.
- Access controls, security safeguards and monitoring measures should be proportionate to risk.
- Personal data and confidential information must be protected from unauthorised access, alteration, disclosure, loss or destruction.
- Compliance with applicable data protection legislation and University policies must be maintained.

- Systems and services should be designed to limit the collection and processing of personal data to what is necessary for the intended purpose.
- Systems processing personal data should support applicable retention, deletion and disposal requirements.

4. Application Principles

Application Principles provide guidance for the selection, development, integration and operation of applications used to deliver University services and capabilities. They support consistency, interoperability, sustainability and alignment with the Enterprise Architecture.

AP-1: Application Portfolio Convergence Statement

Application decisions should progressively align with the University's Enterprise Architecture as systems are introduced, enhanced, replaced or retired. Exceptions may be approved through the appropriate governance process where a clear business justification exists.

Rationale

Convergence enables the University to reduce complexity, improve interoperability, simplify support and ensure consistent delivery of services over time. It allows the architecture to evolve while avoiding unnecessary diversity of technologies and solutions.

Implications

- New applications should align with approved architecture standards and strategic direction.
- Existing systems should be progressively aligned as part of normal lifecycle activities.
- Cloud-based, collaborative and shared-service solutions should be assessed where appropriate.
- Bespoke development should only be undertaken where no suitable alternative exists or where a compelling business case can be demonstrated.
- Architecture exceptions should be documented, justified and approved.

AP-2: Ease of Use

Statement

Applications should be intuitive, accessible and designed to support efficient completion of business tasks.

Rationale

User adoption and productivity are strongly influenced by the usability of applications. Systems that are easy to use reduce training requirements, improve user satisfaction and increase operational effectiveness.

Implications

- User experience should be considered throughout application selection and design.
- Applications should support accessibility and inclusive design principles.
- User interfaces should be consistent wherever practical.
- Training and support requirements should be considered as part of solution selection.
- User feedback should inform application improvements.

AP-3: Application Portability

Statement

Applications should minimise unnecessary dependency on specific technologies, platforms or suppliers wherever practical.

Rationale

Reducing dependency on individual technologies improves flexibility, supports future change and reduces risks associated with technology obsolescence.

Implications

- Open standards should be preferred where practical.
- Data portability should be considered during solution selection.
- Proprietary dependencies should be understood and managed appropriately.
- Long-term maintainability should be considered during procurement and development.

AP-4: Component Simplicity and Reusability

Statement

Applications should be constructed using modular, reusable and maintainable components wherever practical.

Rationale

Reusable components reduce development effort, improve consistency and simplify maintenance and support activities.

Implications

- Existing capabilities should be reused before creating new functionality.
- Components should be loosely coupled and easily maintainable.
- Common business capabilities should be implemented once and shared where appropriate.
- Application architectures should support scalability and flexibility.
- Duplication of functionality should be minimised.

AP-5: Standardised and Reusable Application Interfaces

Statement

Applications should communicate through standardised, documented and reusable interfaces that support integration across the University environment.

Rationale

Standardised interfaces reduce integration complexity, improve maintainability and support information sharing between applications and services.

Implications

- Interfaces should use approved integration standards where practical.
- Application integrations should be documented and governed.
- Interfaces should support security, monitoring and audit requirements.
- Point-to-point integrations should be minimised where more reusable alternatives exist.
- Changes to interfaces should be managed through established change management processes.

5. Technology Principles

Technology Principles provide guidance for the selection, deployment, management and evolution of technology platforms, infrastructure and services used to support the University's operations. These principles promote standardisation, interoperability, efficiency, maintainability and long-term sustainability.

TP-1: Requirements-Based Change

Statement

Changes to technology platforms and infrastructure should be driven by clearly defined business, operational, security, regulatory or architectural requirements.

Rationale

Technology should be implemented to address an identified need rather than as an end in itself. Requirements-based decision-making helps ensure investments deliver value and support the University's strategic objectives.

Implications

- Technology decisions should be supported by documented business, technical and operational requirements.
- Stakeholders should be involved in defining and validating requirements.
- Solutions should be evaluated against both current and anticipated future needs.
- Adoption of new technologies should be justified through measurable benefits and alignment with Enterprise Architecture.
- Requirements should be reviewed periodically to ensure continued relevance.

TP-2: Technology Standardisation

Statement

Technology platforms, infrastructure and services should be standardised wherever practical to improve efficiency, interoperability and supportability.

Rationale

Standardisation reduces complexity, lowers support costs, improves security and enables greater flexibility when integrating systems and services.

Implications

- Approved technology standards should be maintained and periodically reviewed.

- New solutions should align with approved standards where practical.
- Departures from standards should be justified and approved through governance processes.
- Technology diversity should be minimised where it provides no clear business benefit.
- Standardisation should be balanced against innovation and specific business requirements.

TP-3: Responsive Change Management

Statement

Changes to the University's technology environment should be implemented in a timely, controlled and coordinated manner.

Rationale

The technology environment must remain responsive to evolving business requirements while maintaining service stability and operational effectiveness. Delays in implementing necessary changes can limit the University's ability to achieve its objectives.

Implications

- Change management processes should facilitate timely delivery while managing risk appropriately.
- Technology changes should be assessed for architectural, operational and business impacts.
- Architecture artefacts and documentation should be updated following significant changes.
- Appropriate stakeholder engagement should occur before implementing significant changes.
- Where competing priorities exist, decisions should be balanced against Enterprise Architecture principles and institutional priorities.
- Additional resources may be required to support timely implementation of strategic changes.

TP-4: Technology Platform Interoperability

Statement

Technology platforms should support interoperability and integration through the use of approved standards, protocols and interfaces.

Rationale

Interoperability enables information sharing, reduces duplication, improves flexibility and helps protect technology investments. Standardised integration approaches simplify support and improve the University's ability to evolve its digital services.

Implications

- Technology solutions should support approved integration standards wherever practical.
- Open and widely adopted standards should be preferred where appropriate.
- Exceptions to interoperability standards should require documented justification.
- Integration solutions should be maintainable, secure and appropriately governed.
- Standards should be periodically reviewed to ensure continued relevance and effectiveness.
- A formal process should exist for establishing, reviewing and approving technology standards and exceptions.
- Federated identity and centralized authentication services should be used to provide secure, seamless, and consistent user access management.

6. Document Control Summary

Area	Document Information
Author	Information Security Governance Risk & Compliance
Status	Approved
Approved by	David Robinson - Director of Planning, Information and Compliance
Approval date	19 th October 2026
Document Classification	TU Dublin Public