

Architecture Principles

Project Digital Architecture Project

Client Ashfield District Council

Table of Contents

[1 Purpose of this Document 2](#_Toc260231431)

[2 Principle Template 4](#_Toc260231432)

[3 Summary of Principles 5](#_Toc260231433)

[4 Business Principles 7](#_Toc260231434)

[5 Data Principles 7](#_Toc260231435)

[6 Application Principles 10](#_Toc260231436)

[7 Technology Principles 14](#_Toc260231437)

Document Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name:** | Digital Architecture Project |  |  |
| **Prepared By:** | Gavin Harris | **Document Version No:** | 0.2 (draft) |
| **Title:** | Business Principles, Goals, Drivers | **Document Version Date:** | 03/10/2022 |
| **Reviewed By:** |  | **Review Date:** |  |

Distribution List

|  |  |  |
| --- | --- | --- |
| **From** | **Date** | **Email** |
| Gavin Harris | 26/08/2022 | [gavin.harris@ashfield.gov.uk](mailto:gavin.harris@ashfield.gov.uk) |

|  |  |  |  |
| --- | --- | --- | --- |
| **To** | **Action\*** | **Due Date** | **Email** |
| Joanne Froggatt | Review | 13/09/2022 | [joanne.froggatt@ashfield.gov.uk](mailto:joanne.froggatt@ashfield.gov.uk) |
| Andy Slate | Review | 13/09/2022 | [andy.slate@ashfield.gov.uk](mailto:andy.slate@ashfield.gov.uk) |
| Craig Bonar | Approve | 13/09/2022 | [craig.bonar@ashfield.gov.uk](mailto:craig.bonar@ashfield.gov.uk) |
|  |  |  |  |

\* Action Types: Approve, Review, Inform, File, Action Required, Attend Meeting, Other (**please specify**)

Document Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Version Date** | **Revised By** | **Description** |
| 0.1 | 26/08/22 | G Harris | Initial Draft |
| 0.2 | 03/10/22 | G Harris | Revisions to sections 1, 2 and 3. ADC-PRCL-0019 updated. |
|  |  |  |  |

# Purpose of this Document

This document details the Architecture Principles to which Ashfield District Council adheres.

The purpose of this document is to define the Architecture Principles for the relevant information technology architecture and technology domains of Ashfield District Council.

The following need to be considered at the start of any technology or architecture project:

* These principles define the enduring rules that govern the architecture of a desired system, i.e., the target architecture.
* It is mandatory for principles to be considered when designing technology architectures.
* This document contains all the principles for the relevant information technology architecture and technology domains of Ashfield District Council.

The principles contained within this document have been developed after reviewing the existing business principles, business goals, and business drivers that are provided within the previously established strategic and corporate plans of Ashfield District Council. They are organised within this document in the following sections:

4. Business Principles

5. Data Principles

6. Application Principles

7. Technology Principles

# Principle Template

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which the Corporate Services and Transformation section of Ashfield District Council sets about fulfilling its mission.

In their turn, principles may be just one element in a structured set of ideas that collectively define and guide the organization, from values through to actions and results.

Each principle will follow the template below:

|  |  |
| --- | --- |
| **Name** | **<Name of Principle>** |
| **Reference** | <Unique identifier for the principle> |
| **Statement** | The Statement should succinctly and unambiguously communicate the fundamental rule. For the most part, the principles statements for managing information are similar from one organization to the next. It is vital that the principles statement be unambiguous. |
| **Rationale** | The Rationale should highlight the business benefits of adhering to the principle, using business terminology. Point to the similarity of information and technology principles to the principles governing business operations. Also describe the relationship to other principles, and the intentions regarding a balanced interpretation. Describe situations where one principle would be given precedence or carry more weight than another for making a decision. |
| **Implications** | The Implications should highlight the requirements, both for the business and IT, for carrying out the principle – in terms of resources, costs, and activities/tasks. It will often be apparent that current systems, standards, or practices would be incongruent with the principle upon adoption. The impact to the business and consequences of adopting a principle should be clearly stated. The reader should readily discern the answer to: “How does this affect me?” It is important not to oversimplify, trivialize, or judge the merit of the impact. Some of the implications will be identified as potential impacts only, and may be speculative rather than fully analysed. |

# Summary of Principles

The purpose of this section is to provide a list of the high-level principles that are defined in this document.

|  |  |  |
| --- | --- | --- |
| **Reference** | **Name** | **Statement** |
| ADC-PRCL-0001 | [Primacy of Principles](#_Primacy_of_Principles) | The only way we can provide a consistent and measurable level of quality information to decision-makers is if all organizations abide by the principles. |
| ADC-PRCL-0002 | [Compliance with Law](#_Compliance_with_Law) | Enterprise information management processes comply with all relevant laws, policies, and regulations. |
| ADC-PRCL-0003 | [Maximize Benefit to the Enterprise](#_Maximize_Benefit_to) | Information management decisions are made to provide maximum benefit to the enterprise as a whole. |
| ADC-PRCL-0004 | [Protection of Intellectual Property](#_Protection_of_Intellectual) | The enterprise’s Intellectual Property (IP) must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes. |
| ADC-PRCL-0005 | [Information Management is Everybody’s Business](#_Information_Management_is) | All organizations in the enterprise participate in information management decisions needed to accomplish business objectives. |
| ADC-PRCL-0006 | [Business Continuity](#_Business_Continuity) | Enterprise operations are maintained in spite of system interruptions. |
| ADC-PRCL-0007 | [Data is an Asset](#_Data_is_an) | Data is an asset that has value to the enterprise and is managed accordingly. |
| ADC-PRCL-0008 | [Data is Shared](#_Data_is_Shared) | Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organizations. |
| ADC-PRCL-0009 | [Data is an Accessible](#_Data_is_an_1) | Data is accessible for users to perform their functions. |
| ADC-PRCL-0010 | [Data Security](#_Data_Security) | Data is protected from unauthorized use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Name** | **Statement** |
| ADC-PRCL-0011 | [Ease-of-Use](#_Ease-of-Use) | Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand. |
| ADC-PRCL-0012 | [Technology Independence](#_Technology_Independence) | Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms. |
| ADC-PRCL-0013 | [Control Application Proliferation](#_Control_Application_Proliferation) | The diversity and proliferation of applications is controlled to maximize return on investment and minimize the cost of maintaining expertise in multiple operational solutions and processes. |
| ADC-PRCL-0014 | [Requirements-Based Change](#_Requirements-Based_Change) | Only in response to business needs are changes to applications and technology made. |
| ADC-PRCL-0015 | [Responsive Change Management](#_Responsive_Change_Management) | Changes to the enterprise information environment are implemented in a timely manner. |
| ADC-PRCL-0016 | [Control Technical Diversity](#_Control_Technical_Diversity) | Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments. |
| ADC-PRCL-0017 | [Interoperability](#_Interoperability) | Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology. |
| ADC-PRCL-0018 | [Microsoft First](#_Microsoft_First) | Operating systems software and relational database management systems should conform to Microsoft defined standards i.e., Microsoft Windows Server and Microsoft SQL Server etc. |
| ADC-PRCL-0019 | [Agile, innovative, and responsive](#_Agile,_innovative,_and) | All technical solutions will support the organisational goal to embed agile and hybrid working for its staff, using ‘cloud computing’. |
| ADC-PRCL-0020 | [Digital by Design](#_Digital_by_Design) | The enterprise will use digital technologies to design and improve services, thinking more radically about how technology enablement can create simpler, cheaper and better services to customers. |

# Business Principles

|  |  |
| --- | --- |
| **Name** | Primacy of Principles |
| **Reference** | ADC-PRCL-0001 |
| **Statement** | These principles of information management apply to all organizations within the enterprise. |
| **Rationale** | The only way we can provide a consistent and measurable level of quality information to decision-makers is if all organizations abide by the principles. |
| **Implications** | * Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the management of information. * Information management initiatives will not begin until they are examined for compliance with the principles. * A conflict with a principle will be resolved by changing the framework of the initiative. |

|  |  |
| --- | --- |
| **Name** | Compliance with Law |
| **Reference** | ADC-PRCL-0002 |
| **Statement** | Enterprise information management processes comply with all relevant laws, policies, and regulations. |
| **Rationale** | Enterprise policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations. |
| **Implications** | * The enterprise must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data * Education and access to the rules Efficiency, need, and common sense are not the only drivers. Changes in the law and changes in regulations may drive changes in our processes or applications. |

|  |  |
| --- | --- |
| **Name** | Maximize Benefit to the Enterprise |
| **Reference** | ADC-PRCL-0003 |
| **Statement** | Information management decisions are made to provide maximum benefit to the enterprise as a whole. |
| **Rationale** | This principle embodies "service above self". Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organizational perspective. Maximum return on investment requires information management decisions to adhere to enterprise-wide drivers and priorities. No minority group will detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done. |
| **Implications** | * Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage information — technology alone will not bring about this change * Some organizations may have to concede their own preferences for the greater benefit of the entire enterprise * Application development priorities must be established by the entire enterprise for the entire enterprise * Applications components should be shared across organizational boundaries * Information management initiatives should be conducted in accordance with the enterprise plan. Individual organizations should pursue information management initiatives which conform to the blueprints and priorities established by the enterprise. The plan will be changed as needed. * As needs arise, priorities must be adjusted; a forum with comprehensive enterprise representation should make these decisions. |

|  |  |
| --- | --- |
| **Name** | Protection of Intellectual Property |
| **Reference** | ADC-PRCL-0004 |
| **Statement** | The enterprise’s Intellectual Property (IP) must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes. |
| **Rationale** | A major part of an enterprise’s IP is hosted in the IT domain. |
| **Implications** | * While protection of IP assets is everybody’s business, much of the actual protection is implemented in the IT domain — even trust in non-IT processes can be managed by IT processes (email, mandatory notes, etc.). * A security policy, governing human and IT actors, will be required that can substantially improve protection of IP; this must be capable of both avoiding compromises and reducing liabilities. |

|  |  |
| --- | --- |
| **Name** | Information Management is Everybody’s Business |
| **Reference** | ADC-PRCL-0005 |
| **Statement** | All organizations in the enterprise participate in information management decisions needed to accomplish business objectives. |
| **Rationale** | Information users are the key stakeholders, or customers, in the application of technology to address a business need. To ensure information management is aligned with the business, all organizations in the enterprise must be involved in all aspects of the information environment. The business experts from across the enterprise and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of IT. |
| **Implications** | * To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment. * Commitment of resources will be required to implement this principle. |

|  |  |
| --- | --- |
| **Name** | Business Continuity |
| **Reference** | ADC-PRCL-0006 |
| **Statement** | Enterprise operations are maintained in spite of system interruptions. |
| **Rationale** | As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the enterprise must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of operating on alternative information delivery mechanisms. |
| **Implications** | * Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to ensure business function continuity through redundant or alternative capabilities. * Recoverability, redundancy, and maintainability should be addressed at the time of design * Applications must be assessed for criticality and impact on the enterprise mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary. |

# Data Principles

|  |  |
| --- | --- |
| **Name** | Data is an Asset |
| **Reference** | ADC-PRCL-0007 |
| **Statement** | Data is an asset that has value to the enterprise and is managed accordingly. |
| **Rationale** | Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it. |
| **Implications** | * The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data. * Stewards must have the authority and means to manage the data for which they are accountable. * We must make the cultural transition from "data ownership" thinking to "data stewardship" thinking. * The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise personnel and adversely affect decisions across the enterprise. * Part of the role of data steward, who manages the data, is to ensure data Quality Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality — it is probable that policy and procedures will need to be developed for this as well. * A forum with comprehensive enterprise-wide representation should decide on process changes suggested by the steward. * Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing the data must be assigned at the enterprise level. |

|  |  |
| --- | --- |
| **Name** | Data is Shared |
| **Reference** | ADC-PRCL-0008 |
| **Statement** | Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organizations. |
| **Rationale** | Timely access to accurate data is essential to improving the quality and efficiency of enterprise decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The enterprise holds a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organization to efficiently share these islands of data across the organization. Shared data will result in improved decisions since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities. |
| **Implications** | * The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data. * To enable data sharing we must develop and abide by a common set of policies, procedures, and standards governing data management and access for both the short and the long term * For the short term, to preserve our significant investment in legacy systems, we must invest in software capable of migrating legacy system data into a shared data environment * We will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible * For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications * For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the enterprise * Data sharing will require a significant cultural change * This principle of data sharing will continually "bump up against" the principle of data security — under no circumstances will the data sharing principle cause confidential data to be compromised * Data made available for sharing will have to be relied upon by all users to execute their respective tasks * This will ensure that only the most accurate and timely data is relied upon for decision-making. Shared data will become the enterprise-wide "virtual single source" of data. |

|  |  |
| --- | --- |
| **Name** | Data is an Accessible |
| **Reference** | ADC-PRCL-0009 |
| **Statement** | Data is accessible for users to perform their functions. |
| **Rationale** | Wide access to data leads to efficiency and effectiveness in decision-making, and affords a timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved, and consistency of data is improved. |
| **Implications** | * The implication is that there is an education task to ensure that all organizations within the enterprise understand the relationship between value of data, sharing of data, and accessibility to data. * Accessibility involves the ease with which users obtain information * The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of enterprise users and their corresponding methods of access * Access to data does not constitute understanding of the data — personnel should take caution not to misinterpret information * Access to data does not necessarily grant the user access rights to modify or disclose the data This will require an education process and a change in the organizational culture, which currently supports a belief in "ownership" of data by functional units. |

|  |  |
| --- | --- |
| **Name** | Data Security |
| **Reference** | ADC-PRCL-0010 |
| **Statement** | Data is protected from unauthorized use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information. |
| **Rationale** | Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information. Existing laws and regulations require the safeguarding of national security and the privacy of data, while permitting free and open access. Pre-decisional (work-in-progress, not yet authorized for release) information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use. |
| **Implications** | * Aggregation of data, both classified and not, will create a large target requiring review and de-classification procedures to maintain appropriate control Data owners and/or functional users must determine whether the aggregation results in an increased classification level. Appropriate policy and procedures will be needed to handle this review and declassification. Access to information based on a need-to-know policy will force regular reviews of the body of information. * The current practice of having separate systems to contain different classifications needs to be rethought Is there a software solution to separating classified and unclassified data? The current hardware solution is unwieldy, inefficient, and costly. It is more expensive to manage unclassified data on a classified system. Currently, the only way to combine the two is to place the unclassified data on the classified system, where it must remain. * To adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level * Data security safeguards can be put in place to restrict access to "view only" or "never see" Sensitivity labelling for access to pre-decisional, decisional, classified, sensitive, or proprietary information must be determined. * Security must be designed into data elements from the beginning; it cannot be added later Systems, data, and technologies must be protected from unauthorized access and manipulation. Headquarters information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure. * New policies are needed on managing duration of protection for predecisional information and other works-in-progress, in consideration of content freshness |

# Application Principles

|  |  |
| --- | --- |
| **Name** | Ease-of-Use |
| **Reference** | ADC-PRCL-0011 |
| **Statement** | Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand. |
| **Rationale** | The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the enterprise’s integrated information environment. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low. Using an application should be as intuitive as driving a different car. |
| **Implications** | * Applications will be required to have a common "look-and-feel" and support ergonomic requirements; hence, the common look-and-feel standard must be designed and usability test criteria must be developed * Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. * Factors such as linguistics, customer physical infirmities (visual acuity, ability to use keyboard/mouse), and proficiency in the use of technology have broad ramifications in determining the ease-of-use of an application. |

|  |  |
| --- | --- |
| **Name** | Technology Independence |
| **Reference** | ADC-PRCL-0012 |
| **Statement** | Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms. |
| **Rationale** | Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves. Realizing that every decision made with respect to IT makes us dependent on that technology, the intent of this principle is to ensure that Application Software is not dependent on specific hardware and operating systems software. |
| **Implications** | * This principle will require standards which support portability. * For Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) applications, there may be limited current choices, as many of these applications are technology and platform dependent. * Subsystem interfaces will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the Enterprise Architecture. * Middleware should be used to decouple applications from specific software solutions. * As an example, this principle could lead to use of Java, and future Java-like protocols, which give a high degree of priority to platform independence. |

|  |  |
| --- | --- |
| **Name** | Control Application Proliferation |
| **Reference** | ADC-PRCL-0013 |
| **Statement** | The diversity and proliferation of applications is controlled to maximize return on investment and minimize the cost of maintaining expertise in multiple operational solutions and processes. |
| **Rationale** | This principle embodies the terms of "shadow IT” or “rogue IT” because many of these applications are brought into the organization by business users rather than the IT department. This practice will create issues for the enterprise and the IT department as applications are often acquired for user-centric purposes, rather than for attaining the overall mission of the enterprise.  Application proliferation will require centralized control. It is common for enterprises to have application assets dispersed throughout various platforms:   * In the cloud. * In their private data centres. * On premises. * In various SaaS environments.   The enterprise requires a single pane of glass that gives them insight into their entire application portfolio. When they have that kind of control, the principal risks of identity sprawl, data dissipation, and the enlargement of the threat surface will be much easier to manage. Therefore, reducing and rationalising the number of applications across the organisation will make it easier and cheaper to manage the digital infrastructure. |
| **Implications** | * Having many applications at once engenders **identity sprawl**. This forces users into bad password practices—reusing passwords, for example, or not changing them regularly—which then puts the organization at risk. There are two solutions for this:   1. First, deploy single sign-on SSO across your entire app portfolio for centralised identity and access management, to create a consistent user experience. And the more consistent the user experience is, the less likely users will fall for a phishing scam.   2. Multi-factor authentication (MFA) is also critical to guard against a cybercriminal obtaining an employee’s credentials in a username-password access system. With two- or even three-factor authentication, even if one type of authentication is compromised, the applications have extra layers of protection. * Application proliferation will increase the risk of data dissemination and dissipation across multiple applications, different versions of the same data can end up stored in multiple places, and multiple copies means multiple versions of what should be one truth exist, potentially creating confusion. To combat the enterprise should publish guidelines for business-led teams to educate them on data hygiene and the health of data in applications. * Application proliferation will increase the size of the enterprise “threat surface”, which is a significant security risk. With every added layer of complexity, there are more vulnerabilities, and more risk to manage. To fight against these risks and vulnerabilities the enterprise should not only secure its network, but also focus on application security by using technologies such as web application firewalls. * Application development, purchase and implementation priorities must be established by the entire enterprise for the entire enterprise. * Applications components should be shared across organizational boundaries. * As needs arise, priorities must be adjusted; a forum with comprehensive enterprise representation should make decisions around the development, procurement, and implementation of applications to control the expansion in enterprise application portfolios. |

# Technology Principles

|  |  |
| --- | --- |
| **Name** | Requirements-Based Change |
| **Reference** | ADC-PRCL-0014 |
| **Statement** | Only in response to business needs are changes to applications and technology made. |
| **Rationale** | This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the information support — the transaction of business — is the basis for any proposed change. Unintended effects on business due to IT changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs. |
| **Implications** | * Changes in implementation will follow full examination of the proposed changes using the Enterprise Architecture * There is no funding for a technical improvement or system development unless a documented business need exists * Change management processes conforming to this principle will be developed and implemented * This principle may bump up against the responsive change principle. We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs. The purpose of this principle is to keep the focus on business, not technology needs — responsive change is also a business need. |

|  |  |
| --- | --- |
| **Name** | Responsive Change Management |
| **Reference** | ADC-PRCL-0015 |
| **Statement** | Changes to the enterprise information environment are implemented in a timely manner. |
| **Rationale** | If people are to be expected to work within the enterprise information environment, that information environment must be responsive to their needs. |
| **Implications** | * Processes for managing and implementing change must be developed that do not create delays * A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need * If changes are going to be made, the architectures must be kept updated * Adopting this principle might require additional resources * This will conflict with other principles (e.g., maximum enterprise-wide benefit, enterprise-wide applications, etc.) |

|  |  |
| --- | --- |
| **Name** | Control Technical Diversity |
| **Reference** | ADC-PRCL-0016 |
| **Statement** | Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments. |
| **Rationale** | There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs. The business advantages of minimum technical diversity include:   * standard packaging of components. * predictable implementation impact. * predictable valuations and returns. * redefined testing. * utility status, and * increased flexibility to accommodate technological advancements.   Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology. |
| **Implications** | * Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle * Technology choices will be constrained by the choices available within the technology blueprint Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and put in place. * The technology baseline is not being frozen Technology advances are welcomed and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated. |

|  |  |
| --- | --- |
| **Name** | Interoperability |
| **Reference** | ADC-PRCL-0017 |
| **Statement** | Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology. |
| **Rationale** | Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products and facilitate supply chain integration. |
| **Implications** | * Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a nonstandard solution * A process for setting standards, reviewing, and revising them periodically, and granting exceptions must be established * The existing IT platforms must be identified and documented |

|  |  |
| --- | --- |
| **Name** | Microsoft First |
| **Reference** | ADC-PRCL-0018 |
| **Statement** | Operating systems software and relational database management systems should conform to Microsoft defined standards i.e., Microsoft Windows Server and Microsoft SQL Server etc. |
| **Rationale** | Using a Microsoft technology will ensure a consistency across the architecture, improve the ability of the IT Department to manage systems, increase security and help to reduce costs. |
| **Implications** | * Microsoft standards for operating systems and relational database management systems will be utilised unless there is a compelling reason to implement a nonstandard solution. * If Microsoft solutions are already implemented across the enterprise, their built-in functionality and services should be reviewed as part of a requirements management process prior to the procurement and implementation of another vendor solution. * A Microsoft-centric architecture will help an organisation maximise its return on investment of software licencing from this vendor, by utilising the greatest number of services provided by enterprise-level applications such as Microsoft Office 365. |

|  |  |
| --- | --- |
| **Name** | Agile, innovative, and responsive |
| **Reference** | ADC-PRCL-0019 |
| **Statement** | All technical solutions will support the organisational goal to embed agile and hybrid working for its staff, using ‘cloud computing’. |
| **Rationale** | Regardless of whether staff are sitting at a desk in a council office, using a tablet while working from home, or on a smartphone while working in the field, all enterprise systems and applications should work, so they can concentrate on delivering against their designated role. |
| **Implications** | * Mobile applications will be responsive and effortless to use, to ensure that staff can complete their tasks efficiently. * The ubiquitous deployment of ‘cloud computing’ will allow back office and mobile staff to be able to access the same information and online forms as a customer, ensuring consistent and efficient service delivery. * Utilising ‘cloud computing’ will allow the enterprise to minimize investment in technology infrastructure costs in the long-term (i.e., storage, servers, networking etc.) * Utilising ‘cloud computing’ will significantly enhance the business continuity and disaster recovery capabilities of the architecture, supporting [ADC-PRCL-0006](#_Business_Continuity). |

|  |  |
| --- | --- |
| **Name** | Digital by Design |
| **Reference** | ADC-PRCL-0020 |
| **Statement** | The enterprise will use digital technologies to design and improve services, thinking more radically about how technology enablement can create simpler, cheaper and better services to customers. |
| **Rationale** | Using modern technology and automation will reduce duplication of effort, allocate work more quickly and without paperwork and bureaucracy, enabling the enterprise to deliver faster services whilst improving customer satisfaction. |
| **Implications** | * Digital solutions will aspire to be intuitive, straightforward and require minimal user training. * Users will be consulted when design solutions to ensure that the finished product meets their needs and the needs of the business. * All processes and services will be examined from start to finish to determine how they can be simplified, the duplication of data can be prevented, and customer-centricity built in. * Investment in flexible, generic platform technologies that will offer the enterprise core functionality to enable it to digitise processes and redesign services efficiently. * The enterprise will share information and simplify procedures and services to provide better outcomes for its customers and partners. |