System Development Life Cycle Policy for Chicago State University Systems

Policy Statement

Chicago State University's (CSU) Information Technology Department, is responsible for developing, maintaining, and participating in a Systems Development Life Cycle (SDLC) for CSU system development projects. All entities at the University, engaged in systems or software development activities, must follow this policy.

Purpose

The purpose of the CSU System Development and Acceptance Policy is to establish the rules for evaluating, developing, and/or deploying **Information Resources**. CSU is committed to continuously improving the delivery of University ITD projects that are within budget and on schedule to serve the members of the University community and achieve University strategic goals. This policy is designed to help ensure that University ITD projects meet these objectives by establishing a common and consistent set of project management best practices to reduce project risks and increase project successes.

Scope

The CSU System Development and Acceptance Policy applies to individuals who participate in the procurement, development, or operation of any CSU **Information Resource**.

Definitions

- **University-Related Persons / Employee / Staff** are University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University.
- **Associate / "Extra Help", Third-party or 3rd party** is someone officially attached or connected to the College who is not a student or employee (e.g., Extra Help, vendors, interns, temporary staffing, volunteers.)
- **ITD Resources / Information Resources** - include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, security, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
- **Information System** is a major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same

operating characteristics, the same security needs, and reside in the same general operating environment.

- **Information Technology Department** is the individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.
- **Unit** is a college, department, school, program, research center, business service center, or other operating component of the University.
- **A patch** is a software update comprised of code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:
    - Updating software
    - Fixing a software bug
    - Installing new drivers
    - Addressing new security vulnerabilities
    - Addressing software stability issues
- **Patch management cycle** is a part of lifecycle management and is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. Patch management occurs regularly as per the Patch Management Procedure.
- **University Information** is any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.
- **Security Awareness Training** - The formal process for educating employees about the internet and computer security. A good security awareness program should educate employees about institutional policies and procedures for working with information technology (IT).
- **Personally Identifiable Information (PII)** - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
- **Education records under FERPA**, which - with limited exceptions - means all records in any format or medium that are directly related to a student and are maintained by the College.
- **Health Insurance Portability and Accountability Act (HIPAA)** - Demands that all HIPAA covered businesses prevent unauthorized access to “Protected Health Information” or PHI. PHI includes patients' names, addresses, and all information pertaining to the patients' health and payment records.
- **Gramm-Leach-Bliley ACT (GLBA)** - Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or

insurance to explain their information-sharing practices to their customers and to safeguard sensitive data.

- **Functional Lead** - Technical lead point person for a department. Responsibilities include coordination of upgrades, delegating access, and system issues. Acts as a liaison to ITD.
- **The Family Educational Rights and Privacy Act (FERPA)** - a Federal law that protects the privacy of student education records.
- **Information Owner** - is a person responsible for the management and fitness of information elements (also known as critical data elements) - both the content and metadata.
- **Backup** is saving or copying information onto digital storage media.
- **Restore** is performed to return data that has been lost, stolen, or damaged to its original condition or to move data to a new location.
- **Recovery Point Objective** (RPO) is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.
- **Recovery Time Objective** (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.
- **Electronically stored information (ESI)** is the general term for any electronic information stored on any medium (i.e. hard drive, back-up tapes, CDs, DVDs, flash drives, external drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
- **Archive** is defined as the saving of old or unused files on off-line mass storage media for the purpose of releasing on-line storage space.
- **Disaster Recovery** is a combination of the policies, process and procedures related to preparing for recovery of technology infrastructure critical to CSU operations after a natural or human induced event. Disaster recovery focuses on the restoring technology systems that support business functions that fail in the event of a disaster.
- **Bring Your Own Device (BYOD)** refers to employees who bring their personal devices to work, whether laptop, smartphone, or tablet, in order to interface to the corporate network.
- **Risk** - is the potential for damage an action or condition will have on organization's ability to achieve its objectives and/or execute its strategies successfully.
- **Threat** – is the action or condition that conducts or enables the carrying out of potential damage.
- **Vulnerability** – is the weakness that is exploited by the threat causing damage.
- **Impact** – is the magnitude of the damage caused by threat.
- **Likelihood** – is the probability of the threat transpiring.
- **Inherent information security risk** – the information security risk related to the nature of the 3rd-party relationship without accounting for any protections or controls. Inherent risk is sometimes referred to as “impact” and is used to classify third-party relationships as an indicator of what additional due diligence may be warranted.

- **Residual information security risk** – the information security risk remaining once all available applicable protections and controls are accounted for.
- **Internal control** - is any process or action designed to reduce the impact and/or likelihood of a threat.

Responsibility

University-Related Persons / Employee / Staff, students, and other covered individuals (e.g., **Associate / "Extra Help", Third-party or 3rd party** , etc.) that perform any type of software or systems development work under the auspices of the University.

In the event a CSU Department or Unit chooses to seek an exemption from this policy, that Department or Unit will prepare a risk assessment that details the residual risk associated with such an exemption. This risk assessment will be reviewed by the ITD Information Security Risk Review Group, subject to the risk governance framework described in the CSU Information Security Risk Management Policy.

Policy

General

- Applications created or deployed inside the CSU IT environment must follow a standardized application lifecycle established by management.
- Applications should be actively maintained and have periodic updates to address vulnerabilities. If an application is no longer maintained by the developer or another party, it must be evaluated for replacement.
- At the onset of the acquisition or design phase of an application deployment, the CSU ITD Leader (or a delegate) must provide a list of required security controls based on the Secure Software Development Lifecycle Standard.
- Development, testing, and operational environments must be separated.
- Separation of duties must exist between personnel assigned to the development/test environments and those assigned to the production environment.
- Changes to the system must be made according to the Change Control Policy.
- When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
- The production data source must be sanitized before use in development or test environment and production/test access controls must comply with production standards.
- Test data and accounts must be removed before a production system becomes active.

Program / Project Management

Definition of a Project

The definition of a project for this policy is:

- A temporary endeavor with a beginning and an end.
- Creates or enhances a unique University ITD product or service or prepares members of the University community for the shutdown of an existing IT service.

- Is progressively elaborated – the project requirements, plans, and schedule become increasingly detailed over time as the project is better understood.
- Requires the participation of four or more project team members for a duration of one month or greater.

Guidelines and Procedures

ITD projects typically undergo several steps in its execution, including significant upgrades.

Phases of an SDLC Project

CSU's System Development Life Cycle includes six phases, during which defined work products and documents are created, reviewed, refined, and approved. Not every project will require that the phases be subsequently executed and may be tailored to accommodate the unique aspects of a projects. These phases are described in more detail in the following paragraphs.

Initiation Phase

The Initiation Phase begins when management determines that it is necessary to enhance a business process through the application of information technology. The purposes of the Initiation Phase are to:

- Identify and validate an opportunity to improve business accomplishments of the University or a deficiency related to a business need
- Identify significant assumptions and constraints on solutions to that need
- Recommend the exploration of alternative concepts and methods to satisfy the need.

Feasibility Phase

The Feasibility Phase is the initial investigation, or brief study of the problem to determine whether the systems project should be pursued. A feasibility study established the context through which the project addresses the requirements expressed in Business Case and investigates the practicality of a proposed solution. The feasibility study is used to determine if the project should get the go-ahead. If the project is to proceed, the feasibility study will produce a project plan and budget estimates for the future stages of development.

Requirements Analysis Phase

This phase formally defines the detailed functional user requirements using high-level requirements identified in the Initiation and Feasibility Phases. The requirements are defined in this phase to a level of detail sufficient for systems design to proceed. They need to be measurable, testable, and relate to the business need or opportunity identified in the Initiation Phase. The purposes of this phase are to:

- Complete business process reengineering of the functions to be supported, e.g., verify what information drives the business process, what information is generated, who generates it, where does the information go, and who processes it.
- Develop detailed data and process models including system inputs and outputs.
- Develop the test and evaluation requirements that will be used to determine acceptable system performance.

Design Phase

During this phase, the system is designed to satisfy the functional requirements identified in the previous phase. Since problems in the design phase can be very expensive to solve in later stages of the software development, a variety of elements are considered in the design to mitigate risk. These include:

- Identifying potential risks and defining mitigating design features
- Performing a security risk assessment
- Developing a conversion plan to migrate current data to the new system • Determining the operating environment
- Defining major subsystems and their inputs and outputs
- Allocating processes to resources

Development Phase

Effective completion of the previous stages is a key factor in the success of the Development phase. The Development phase consists of:

- Translating the detailed requirements and design into system components
- Testing individual elements (units) for usability
- Preparing for integration and testing of the IT system.

Integration, system, security, and user acceptance testing is conducted during this phase as well. The user, with those responsible for quality assurance, validates that the functional requirements are met by the newly developed or modified system.

Implementation Phase

This phase is initiated after the system has been tested and accepted by the user. In this phase, the system is installed to support the intended business functions. System performance is compared to performance objectives established during the planning phase. Implementation may include user notification, user training, installation of hardware, installation of software onto production computers, and integration of the system into daily work processes. This phase continues until the system is operating in production in accordance with the defined user requirements.

Operations and Maintenance

The system operation is ongoing. The system is monitored for continued performance in accordance with user requirements and needed system modifications are incorporated. Operations continue as long as the system responds to the organization's needs. When modifications are identified, the system may reenter the planning phase.

Conditions that Invoke the Application of the Policy

This policy applies to all CSU ITD projects as defined above that meet any of the following conditions:

- Has a project budget of $XXX,XXX or more including University staff expenses.

- Requires an ongoing operational budget of $XXX,XXX or more annually for the service(s) created by the project.
- Has a 5-year lifecycle cost including both the project and ongoing operational expense that is estimated to be $X,XXX,XXX or greater.

Requirements of the Policy

If a University ITD project meets any of the conditions that invoke the policy, the project must utilize ITD approved project management practices including, roles, and documentation that are defined in the "Required Project Documents" section of this policy.

Required Project Roles

The University approves the use of the following project management roles and requires the specified project roles to be held for the duration of the project.

Project Manager

A project must have a project manager and at least one project sponsor for the duration of the project. The project manager is the person responsible for the overall project management processes and the successful initiation, planning, execution, monitoring, and closing of the project. The project manager reports to the project sponsor for the duration of the project.

Project Sponsor

The sponsor is the person who has the highest level of authority over the project. The sponsor provides the project team with high-level direction for the project and is ultimately responsible for the project's success. The sponsor is also responsible for project funding and resolving critical organizational issues required for the success of the project. The sponsor approves the project charter, scope changes, and major deliverables.

Required Project Documents

The project manager must create and maintain the following documents for each University project subject to the policy:

- A project charter that defines the project's business case, scope, goals, metrics of project success, major milestones, high-level risks, and identifies the key stakeholders and the project team members including the roles they hold. The charter must define the responsibilities of the project manager and the sponsor. The project cannot proceed until the sponsor approves the charter and accepts the responsibilities of their position by signing the charter.
- A budget that estimates the cost of conducting the project and the first five years of operation.
- A project plan that describes the work to be performed including an estimated schedule of when the work will be completed by whom and identifies dependencies between work tasks.
- A change management plan that describes the training and communication activities that will be conducted to help faculty, students, and staff use the new service(s) created by the project.

- A risk plan that identifies project risks and planned responses to manage the risks which are mostly likely to occur and to have a significant adverse impact on the project.
- Project status reports that are created by the project manager and sent to the project sponsor on at least a monthly basis.

Secure Development

- All software development personnel must receive training in writing secure code for their specific development environment.
- A Secure Software Development Lifecycle Standard must be developed and implemented.
- Access to program source code should be restricted based on principle of least privilege.
- For applications that store or transmit confidential information controls must be implemented to limit output to minimum necessary as defined by the user.
- Any outsourced software development should comply with the Secure Software Development Lifecycle Standard recommendations.
- Modifications to externally developed software packages must be limited to necessary changes and all changes should be strictly controlled.

System Acceptance

- Acceptance criteria must be provided by the application owner and should specify:
    - The operational and functional requirements of the application.
    - Performance and capacity requirements.
- All acceptance criteria must be satisfied before any application can move into a production environment.

Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU ITD Approval Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted by ITD.

Enforcement

This System Development Life Cycle Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between CSU policies, they must be brought to the attention of CSU for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

References

- NIST CSF: PR.AT, PR.DS, PR.IP
- The Illinois State Auditing Act (30 ILCS 5/3-2.4)

Version History

Version	Modified Date	Next Review	Approved Date	Approved By	Comments
1.0	11/3/2022	11/1/2023	11/6/2022	Donna Hart	