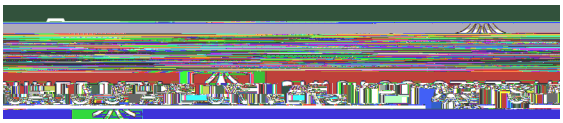
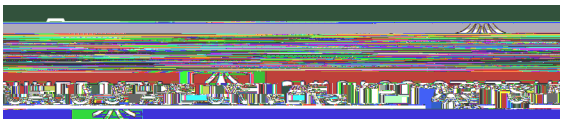
CSU Information Security Policy



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
  - Addressipdanclude, bude, b

SDLC



- 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.

- 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.

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

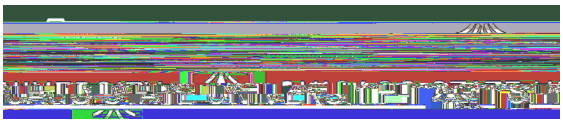
The system operation is ongoing. The system is monitored for continued performance in accordance with user requirements and needed system modifications are incorporated. Operations continue as long as the system responds to the organization's needs. When modifications are identified, the system may reenter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

Conditions that Invoke the Application of the Policy

This policy applies to all CSU IT 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 $X,XXX or more annually for the 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 actions 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)