



Information Privacy and Security (IPAS) Phase II Project Activity

While much of the activity associated with this project phase will need to follow the high priority activity of Phase I, there will be some activity overlap when activities of Phase I relate to the tasks of Phase II.

1. Define and implement improved distributed information privacy and security risk assessment processes.
2. Examine and recommend changes to distributed College and unit Security and Privacy policies.
3. Establish an archive for all Policies in Security and Privacy.
4. Define a formal University-wide security and privacy training strategy for distributed IT staff to include mandatory initial courses and ongoing professional development courses thereafter.
5. Examine and refine security and privacy job descriptions to formalize qualifications for employees.
6. Define and implement a distributed system and software development life cycle that includes security as an integral part of the process in all phases.
7. Examine the current security and privacy organizational structure and define improvements that would enhance both distributed and central security and privacy functions.
8. Define and implement a more effective distributed compliance and enforcement strategy with regard to existing or enhanced/future security and privacy needs.
9. Examine and recommend any necessary changes to staffing and funding levels for the central and distributed privacy and security functions.
10. In coordination with the Telecommunications and Networking Services (TNS) unit of Information Technology Services (ITS), examine and recommend (if required) architectural changes to the University's integrated backbone network that would enable easier introduction of technical security solutions.
11. Examine the feasibility of Network Access Control technologies, either centrally controlled and managed or unit-controlled.

12. Examine and implement more effective log aggregation and monitoring strategies.
13. Examine and implement, as needed, additional training, awareness and technical measures for the average user of technology (faculty, student, staff) in the security/privacy areas.
14. Examine the feasibility of implementing performance-based incentives in the OHR system such that staff attaining a particular level of security proficiency are officially recognized.