Lecture 4: April 6, 2026

Reading: *text*, §14, [1] **Due:** Homework 1, due April 10, 2026

1. Greetings and felicitations!
2. Principles of secure design (*con't.*)
   (a) Simplicity and restrictiveness
   (b) Principle of open design
   (c) Principle of separation of privilege
   (d) Principle of least common mechanism
   (e) Principle of least astonishment
3. Privacy
   (a) What it is
   (b) Relationship to confidentiality
4. Principles of privacy by design
   (a) Proactive not reactive; preventive not remedial
   (b) Privacy as the default setting
   (c) Privacy embedded into design
   (d) Full functionality — positive-sum, not zero-sum
   (e) End-to-end security — full lifecycle protection
   (f) Visibility and transparency — keep it open
   (g) Respect for user privacy — keep it user-centric
5. Access Control Matrix

References

[1] A. Cavoukian, "Privacy by Design: The Seven Foundational Principles," *The Sedona Conference Institute* (May 2010). URL: https://www.thesedonaconference.org/sites/default/files/conference_papers/Recommended%20%5B08b%5D%20Privacy%20By%20Design_Cavoukian.pdf.