Computer Crime and Privacy Laws Cheat Sheet

Law	Type	Summary
Computer Fraud and Abuse Act (CFAA)	Federal	Is a law passed by the United States Congress in 1986 intended to address unauthorized access and use of computer systems and computer networks. It was amended in 1994, 1996 and in 2001 by the USA PATRIOT Act.
Health Insurance Portability and Accountability Act (HIPAA)	Federal	This law meets minimum standards of due care to provide confidentiality and protection for patient physical and individually identifiable electronic Protected Health Information (e-PHI).
California Government Code 8314.5	California	This law deals with the definition of "obscene matter" and how accessing, viewing, or downloading this obscene matter is dealt with.
California Penal Code 502	California	This law deals with unauthorized access to computers, computer systems and computer data
California Penal Code 646.9	California	This law deals with cyberstalking and harassment.
California Code of Regulations, Title V, Sections 42396 - 42396.5	California	Title V of the California Code of Regulations, specifically sections 42396 - 42396.5 addresses privacy and principles of personal information management applicable to the California State University.
California Information Privacy Act	California	The California Security Breach Information Act (SB-1386) is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is acquired by an unauthorized person. The Act, which went into effect July 1, 2003, was created to help stem the increasing incidence of identity theft. Found in the California Civil Code (Sections 1798.29).
California Senate Bill 25 (SB 25)	California	SB 25 extends those Social Security number restrictions to all government agencies, including public colleges and universities. Under SB 25, public entities will have to ensure that Social Security numbers don't get posted or displayed on any printed material, or used on identification cards.
Fair and Accurate Credit Transactions Act (FACTA)	Federal	In 2003, Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which required "creditors" to adopt policies and procedures to prevent identity theft. These requirements are described in section 114 of FACTA and are known as the "Red Flags Rule". The Red Flags Rule applies to financial institutions and "creditors" that offer or maintain accounts that provide for multiple transactions primarily for personal, family, or household purposes. Institutions are considered creditors if they provide goods or services that are not fully paid for in advance or allow individuals to defer payment for goods or services.

Family Educational Rights and Privacy Act (FERPA)	Federal	Responsible for Enacted in 1974, FERPA protects the privacy of student education records and affords students (or parents if the student is a minor) certain rights with respect to the student's "education records." More information about the SJSU FERPA program can be found at: http://www.sjsu.edu/studentconduct/docs/FERPA.pdf
Gramm-Leach-Bliley Act (GLBA)	Federal	Enacted in 1999, the GLBA requires financial institutions to carefully protect customers' financial information. Universities are "financial institutions" by virtue of their loan servicing and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) "safeguarding" rules and (2) privacy rules. All personally identifiable financial information from students, parents, and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure.
Information Practices Act of 1977 (IPA)	California	Found in the California Civil Code (Sections 1798.14-1798.23), the IPA requires State agencies to record only personal information that is relevant and necessary to accomplish the purpose of the agency. Additionally, the agency should collect personal information directly from the individual who is the subject of the information rather than from any other source.
Payment Card Industry Data Security Standard (PCI DSS)	Security Standards Council (SSC)	The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. It applies to American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International.