CHAPTER TWO

ACADEMIC AFFAIRS

240 INFORMATION TECHNOLOGY SERVICES

Information Technology Services encompasses Information Technology Services and the Office of the CIO. OCIO functions include information security, policy development and compliance, strategic planning and process development, technology architecture and planning, quality assurance and assessment, and IT governance.

240.1 University IT Policies

240.1.1 Under the direction of the vice provost/chief information officer, Information Technology Services is responsible for coordinating the development, dissemination, implementation, interpretation, and enforcement of information security, resource and technology-related policies, standards, guidelines and procedures.

240.1.2 Policies are high-level statements of principle that provide scope and direction to the campus. The policies are “technology agnostic” in that they are unbiased toward the use of specific technology tools, hardware or software.

240.1.3 Standards establish specific criteria, roles and responsibilities, and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and provide a basis for verifying compliance through audits and assessments.

240.1.4 Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

240.1.5 Practices consist of one or more series of interrelated steps to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to complete the process.

240.2 Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives.

240.3 Information Security Program
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
CHAPTER TWO

ACADEMIC AFFAIRS

240  INFORMATION TECHNOLOGY SERVICES

Information Technology Services encompasses Information Technology Services and the Office of the CIO. OCIO functions include information security, policy development and compliance, strategic planning and process development, technology architecture and planning, quality assurance and assessment, and IT governance.

240.1  University IT Policies

240.1.1  Under the direction of the vice provost/chief information officer, Information Technology Services is responsible for coordinating the development, dissemination, implementation, interpretation, and enforcement of information security, resource and technology-related policies, standards, guidelines and procedures.

240.1.2  Policies are high-level statements of principle that provide scope and direction to the campus. The policies are “technology agnostic” in that they are unbiased toward the use of specific technology tools, hardware or software.

240.1.3  Standards establish specific criteria, roles and responsibilities, and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and provide a basis for verifying compliance through audits and assessments.

240.1.4  Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

240.1.5  Practices consist of one or more series of interrelated steps to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to complete the process.

240.2  Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives.

240.3  Information Security Program
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
CHAPTER TWO

ACADEMIC AFFAIRS

240 INFORMATION TECHNOLOGY SERVICES

Information Technology Services encompasses Information Technology Services and the Office of the CIO. OCIO functions include information security, policy development and compliance, strategic planning and process development, technology architecture and planning, quality assurance and assessment, and IT governance.

240.1 University IT Policies

240.1.1 Under the direction of the vice provost/chief information officer, Information Technology Services is responsible for coordinating the development, dissemination, implementation, interpretation, and enforcement of information security, resource and technology-related policies, standards, guidelines and procedures.

240.1.2 Policies are high-level statements of principle that provide scope and direction to the campus. The policies are “technology agnostic” in that they are unbiased toward the use of specific technology tools, hardware or software.

240.1.3 Standards establish specific criteria, roles and responsibilities, and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and provide a basis for verifying compliance through audits and assessments.

240.1.4 Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

240.1.5 Practices consist of one or more series of interrelated steps to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to complete the process.

240.2 Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives.

240.3 Information Security Program
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
CHAPTER TWO
ACADEMIC AFFAIRS

240  INFORMATION TECHNOLOGY SERVICES

Information Technology Services encompasses Information Technology Services and the Office of the CIO. OCIO functions include information security, policy development and compliance, strategic planning and process development, technology architecture and planning, quality assurance and assessment, and IT governance.

240.1  University IT Policies

240.1.1  Under the direction of the vice provost/chief information officer, Information Technology Services is responsible for coordinating the development, dissemination, implementation, interpretation, and enforcement of information security, resource and technology-related policies, standards, guidelines and procedures.

240.1.2  Policies are high-level statements of principle that provide scope and direction to the campus. The policies are “technology agnostic” in that they are unbiased toward the use of specific technology tools, hardware or software.

240.1.3  Standards establish specific criteria, roles and responsibilities, and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and provide a basis for verifying compliance through audits and assessments.

240.1.4  Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

240.1.5  Practices consist of one or more series of interrelated steps to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to complete the process.

240.2  Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives.

240.3  Information Security Program
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
CHAPTER TWO

ACADEMIC AFFAIRS

240 INFORMATION TECHNOLOGY SERVICES

Information Technology Services encompasses Information Technology Services and the Office of the CIO. OCIO functions include information security, policy development and compliance, strategic planning and process development, technology architecture and planning, quality assurance and assessment, and IT governance.

240.1 University IT Policies

240.1.1 Under the direction of the vice provost/chief information officer, Information Technology Services is responsible for coordinating the development, dissemination, implementation, interpretation, and enforcement of information security, resource and technology-related policies, standards, guidelines and procedures.

240.1.2 Policies are high-level statements of principle that provide scope and direction to the campus. The policies are “technology agnostic” in that they are unbiased toward the use of specific technology tools, hardware or software.

240.1.3 Standards establish specific criteria, roles and responsibilities, and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and provide a basis for verifying compliance through audits and assessments.

240.1.4 Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

240.1.5 Practices consist of one or more series of interrelated steps to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to complete the process.

240.2 Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives.

240.3 Information Security Program
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
CHAPTER TWO

ACADEMIC AFFAIRS

240 INFORMATION TECHNOLOGY SERVICES

Information Technology Services encompasses Information Technology Services and the Office of the CIO. OCIO functions include information security, policy development and compliance, strategic planning and process development, technology architecture and planning, quality assurance and assessment, and IT governance.

240.1 University IT Policies

240.1.1 Under the direction of the vice provost/chief information officer, Information Technology Services is responsible for coordinating the development, dissemination, implementation, interpretation, and enforcement of information security, resource and technology-related policies, standards, guidelines and procedures.

240.1.2 Policies are high-level statements of principle that provide scope and direction to the campus. The policies are “technology agnostic” in that they are unbiased toward the use of specific technology tools, hardware or software.

240.1.3 Standards establish specific criteria, roles and responsibilities, and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and provide a basis for verifying compliance through audits and assessments.

240.1.4 Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

240.1.5 Practices consist of one or more series of interrelated steps to achieve a specific goal designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to complete the process.

240.2 Policy development is driven by CSU policies and directives, new legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives.

240.3 Information Security Program
The Cal Poly Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of Cal Poly information assets. In accordance with the CSU Information Security Policy, the Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of Cal Poly, violate individual privacy rights, and possibly constitute a criminal act.

Cal Poly’s information security practices must comply with a variety of federal and state laws, and CSU policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g. social security number, driver’s license number), personal financial information (e.g. credit card numbers), medical information, and confidential student information.

240.3.1 The purpose of the Information Security Program is to:

240.3.1.1 Document roles and responsibilities for the Information Security Program;

240.3.1.2 Provide for the confidentiality, integrity, and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g. paper or electronic);

240.3.1.3 Document risk-management strategies to identify and mitigate threats and vulnerabilities to level one and level two information assets as defined in the Cal Poly Information Classification and Handling Standard;

240.3.1.4 Document incident response strategies;

240.3.1.5 Document strategies for ongoing security awareness and training; and

240.3.1.6 Comply with applicable laws, regulations, Cal Poly and CSU policies.

240.3.1.7 It is the collective responsibility of all users (i.e., any person or resource that accesses, uses or manages information assets) to ensure the:

240.3.1.8 Confidentiality of protected information from unauthorized access;

240.3.1.9 Integrity and availability of information stored on or processed by Cal Poly information systems; and
240.3.1.10 Campus compliance with applicable laws, regulations and policies governing information security and privacy protection.

240.3.2 The Information Security Program and its related standards and practices guide the secure use of campus information assets to meet the University’s core mission and academic and administrative goals. The program may be augmented, but neither supplanted nor diminished, by additional policies and standards.

240.3.3 This policy covers: policy development and management; organization and governance; risk management, assessment and planning; privacy of personal information; personnel security; awareness and training; managing third parties; information technology security; configuration management; change control; access control; information asset management; information systems acquisition, development and maintenance; incident management; physical security; business continuity and disaster recovery; and compliance and enforcement.

The Information Security Program applies to:

240.3.3.1 Centrally and departmentally managed campus information assets;

240.3.3.2 All users employed by Cal Poly, third parties and affiliated users, or any other person with access to Cal Poly’s network resources or information assets. This includes computing devices not owned by Cal Poly that may access or store protected information;

240.3.3.3 All categories of information, regardless of the physical or electronic medium in which the information asset is held or transmitted; and

240.3.3.4 Information technology facilities, applications, hardware systems and network resources owned or managed by Cal Poly. This includes third party service-provider systems that access or store Cal Poly’s protected information.

240.3.4 Auxiliary organizations, external businesses and organizations that use campus information assets must operate those assets in conformity with the Information Security Program.

240.3.5 Cal Poly retains ownership or stewardship of information assets owned (or managed) by or entrusted to Cal Poly. Cal Poly reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the
240.3.1.10 Campus compliance with applicable laws, regulations and policies governing information security and privacy protection.

240.3.2 The Information Security Program and its related standards and practices guide the secure use of campus information assets to meet the University’s core mission and academic and administrative goals. The program may be augmented, but neither supplanted nor diminished, by additional policies and standards.

240.3.3 This policy covers: policy development and management; organization and governance; risk management, assessment and planning; privacy of personal information; personnel security; awareness and training; managing third parties; information technology security; configuration management; change control; access control; information asset management; information systems acquisition, development and maintenance; incident management; physical security; business continuity and disaster recovery; and compliance and enforcement.

The Information Security Program applies to:

240.3.3.1 Centrally and departmentally managed campus information assets;

240.3.3.2 All users employed by Cal Poly, third parties and affiliated users, or any other person with access to Cal Poly’s network resources or information assets. This includes computing devices not owned by Cal Poly that may access or store protected information;

240.3.3.3 All categories of information, regardless of the physical or electronic medium in which the information asset is held or transmitted; and

240.3.3.4 Information technology facilities, applications, hardware systems and network resources owned or managed by Cal Poly. This includes third party service-provider systems that access or store Cal Poly’s protected information.

240.3.4 Auxiliary organizations, external businesses and organizations that use campus information assets must operate those assets in conformity with the Information Security Program.

240.3.5 Cal Poly retains ownership or stewardship of information assets owned (or managed) by or entrusted to Cal Poly. Cal Poly reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the
campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are intended to protect the confidentiality, integrity and availability of information, and are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

240.3.6 To safeguard and secure campus information and information resources, all users and campus departments are expected to adhere to this policy and related standards where applicable, and to report suspected violations in accordance with established practices.

240.3.7 The full text of the Information Security Program (ISP) is maintained on Cal Poly’s Information Security website and by reference is incorporated into this section of CAP.

240.4 Responsible Use Policy

240.4.1 The principal concern of this policy is the effective and efficient use of information technology (IT) resources such that the resources are used in a manner that does not impair or impede their use by others in their pursuit of the mission of the University. The policy is intended to ensure:

240.4.1.1 The integrity, reliability, and good performance of University resources;

240.4.1.2 That the user community (as defined in 242.2) operates according to established policies and applicable laws;

240.4.1.3 That these resources are used for their intended purposes; and

240.4.1.4 That appropriate measures are in place to assure the policy is honored.

240.4.2 IT resources are provided to support the University’s mission of education, research and service. To ensure that these shared and finite resources are used effectively to further the University’s mission, each user has the responsibility to:

240.4.2.1 Use the resources appropriately and efficiently;

240.4.2.2 Respect the freedom and privacy of others;

240.4.2.3 Protect the stability and security of the resources; and

240.4.2.4 Understand and fully abide by established University policies and applicable public laws.
240.3.1.10 Campus compliance with applicable laws, regulations and policies governing information security and privacy protection.

240.3.2 The Information Security Program and its related standards and practices guide the secure use of campus information assets to meet the University’s core mission and academic and administrative goals. The program may be augmented, but neither supplanted nor diminished, by additional policies and standards.

240.3.3 This policy covers: policy development and management; organization and governance; risk management, assessment and planning; privacy of personal information; personnel security; awareness and training; managing third parties; information technology security; configuration management; change control; access control; information asset management; information systems acquisition, development and maintenance; incident management; physical security; business continuity and disaster recovery; and compliance and enforcement.

The Information Security Program applies to:

240.3.3.1 Centrally and departmentally managed campus information assets;

240.3.3.2 All users employed by Cal Poly, third parties and affiliated users, or any other person with access to Cal Poly’s network resources or information assets. This includes computing devices not owned by Cal Poly that may access or store protected information;

240.3.3.3 All categories of information, regardless of the physical or electronic medium in which the information asset is held or transmitted; and

240.3.3.4 Information technology facilities, applications, hardware systems and network resources owned or managed by Cal Poly. This includes third party service-provider systems that access or store Cal Poly’s protected information.

240.3.4 Auxiliary organizations, external businesses and organizations that use campus information assets must operate those assets in conformity with the Information Security Program.

240.3.5 Cal Poly retains ownership or stewardship of information assets owned (or managed) by or entrusted to Cal Poly. Cal Poly reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the
240.3.1.10 Campus compliance with applicable laws, regulations and policies governing
information security and privacy protection.

240.3.2 The Information Security Program and its related standards and practices guide
the secure use of campus information assets to meet the University’s core mission
and academic and administrative goals. The program may be augmented, but
neither supplanted nor diminished, by additional policies and standards.

240.3.3 This policy covers: policy development and management; organization and
governance; risk management, assessment and planning; privacy of personal
information; personnel security; awareness and training; managing third parties;
information technology security; configuration management; change control;
access control; information asset management; information systems acquisition,
development and maintenance; incident management; physical security; business
continuity and disaster recovery; and compliance and enforcement.

The Information Security Program applies to:

240.3.3.1 Centrally and departmentally managed campus information assets;

240.3.3.2 All users employed by Cal Poly, third parties and affiliated users, or any other
person with access to Cal Poly’s network resources or information assets. This
includes computing devices not owned by Cal Poly that may access or store
protected information;

240.3.3.3 All categories of information, regardless of the physical or electronic medium in
which the information asset is held or transmitted; and

240.3.3.4 Information technology facilities, applications, hardware systems and network
resources owned or managed by Cal Poly. This includes third party service-
provider systems that access or store Cal Poly’s protected information.

240.3.4 Auxiliary organizations, external businesses and organizations that use campus
information assets must operate those assets in conformity with the Information
Security Program.

240.3.5 Cal Poly retains ownership or stewardship of information assets owned (or
managed) by or entrusted to Cal Poly. Cal Poly reserves the right to limit access
to its information assets and to use appropriate means to safeguard its data,
preserve network and information system integrity, and ensure continued delivery
of services to users. This can include, but is not limited to: monitoring
communications across campus network services; monitoring actions on the
campus information systems; checking information systems attached to the
campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are intended to protect the confidentiality, integrity and availability of information, and are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

240.3.6 To safeguard and secure campus information and information resources, all users and campus departments are expected to adhere to this policy and related standards where applicable, and to report suspected violations in accordance with established practices.

240.3.7 The full text of the Information Security Program (ISP) is maintained on Cal Poly’s Information Security website and by reference is incorporated into this section of CAP.

240.4 Responsible Use Policy

240.4.1 The principal concern of this policy is the effective and efficient use of information technology (IT) resources such that the resources are used in a manner that does not impair or impede their use by others in their pursuit of the mission of the University. The policy is intended to ensure:

240.4.1.1 The integrity, reliability, and good performance of University resources;

240.4.1.2 That the user community (as defined in 242.2) operates according to established policies and applicable laws;

240.4.1.3 That these resources are used for their intended purposes; and

240.4.1.4 That appropriate measures are in place to assure the policy is honored.

240.4.2 IT resources are provided to support the University’s mission of education, research and service. To ensure that these shared and finite resources are used effectively to further the University’s mission, each user has the responsibility to:

240.4.2.1 Use the resources appropriately and efficiently;

240.4.2.2 Respect the freedom and privacy of others;

240.4.2.3 Protect the stability and security of the resources; and

240.4.2.4 Understand and fully abide by established University policies and applicable public laws.
240.4.3 This policy applies to all users and all IT resources and services provided by the University in support of Cal Poly’s core academic mission and to enable users to access, communicate, store, retrieve and transmit data. It also relates to the impact and consequences such actions of individuals or groups may have on the IT infrastructure and identifies suitable conduct where such conduct is known or described as part of law or acceptable practice. Upon initial access and annually thereafter, users must acknowledge that they have read and agree to abide by the policy.

240.4.4 Additional use policies and terms and conditions may be in place for specific campus resources or non-University resources that support Cal Poly’s mission. Users must become familiar with any policies when agreeing to use such resources.

240.4.5 Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, in much the same way as a driver’s license is granted, and requires that individual users know what is expected of them and that they act responsibly.

240.4.6 Users must respect the rights of other users; respect the confidentiality, integrity and availability of the systems and related physical resources they have access to; and observe all relevant laws, regulations, and contractual obligations. (Integrity refers to an IT asset performing its intended functions in an unimpaired manner, i.e., free from deliberate or inadvertent unauthorized manipulation.)

240.4.7 Users are responsible for staying informed of applicable laws and regulations governing the use of IT resources and services and, when unsure, to seek advice and guidance from the full policy as posted and issued from the appropriate University officials assigned to advise on such matters.

240.4.8 Policy provisions include, but are not limited to, authorized use/access; data security, confidentiality and privacy; electronic information retention and disclosure; network and system integrity; commercial use; political advocacy; harassment; copyright; trademark and patents; electronic communications; and Internet/Web use and accessibility of digital content.

240.4.9 All existing laws (federal and state) and University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks (e.g. malware), but also those that apply generally to personal conduct (e.g. harassment).

240.4.10 Compliance and Enforcement
This policy applies to all users and all IT resources and services provided by the University in support of Cal Poly’s core academic mission and to enable users to access, communicate, store, retrieve and transmit data. It also relates to the impact and consequences such actions of individuals or groups may have on the IT infrastructure and identifies suitable conduct where such conduct is known or described as part of law or acceptable practice. Upon initial access and annually thereafter, users must acknowledge that they have read and agree to abide by the policy.

Additional use policies and terms and conditions may be in place for specific campus resources or non-University resources that support Cal Poly’s mission. Users must become familiar with any policies when agreeing to use such resources.

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, in much the same way as a driver’s license is granted, and requires that individual users know what is expected of them and that they act responsibly.

Users must respect the rights of other users; respect the confidentiality, integrity and availability of the systems and related physical resources they have access to; and observe all relevant laws, regulations, and contractual obligations. (Integrity refers to an IT asset performing its intended functions in an unimpaired manner, i.e., free from deliberate or inadvertent unauthorized manipulation.)

Users are responsible for staying informed of applicable laws and regulations governing the use of IT resources and services and, when unsure, to seek advice and guidance from the full policy as posted and issued from the appropriate University officials assigned to advise on such matters.

Policy provisions include, but are not limited to, authorized use/access; data security, confidentiality and privacy; electronic information retention and disclosure; network and system integrity; commercial use; political advocacy; harassment; copyright; trademark and patents; electronic communications; and Internet/Web use and accessibility of digital content.

All existing laws (federal and state) and University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks (e.g. malware), but also those that apply generally to personal conduct (e.g. harassment).

Compliance and Enforcement
240.4.11 Users may be held accountable for their conduct under any applicable University policies, procedures or collective bargaining agreements. Enforcement will be based upon receipt of one or more formal complaints about a specific incident or through discovery of a possible violation in the normal course of administering IT resources and services. Complaints alleging serious misuse will be directed to those responsible for taking appropriate disciplinary action. Appeals of University actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes.

240.4.12 First offenses and minor infractions are generally resolved informally by the entity responsible for the resource. Repeat offenses and serious incidents may lead to formal disciplinary action up to and including dismissal or termination. Misuse may result in the loss of computing privileges and prosecution under applicable civil and criminal statutes.

240.4.13 The full text of the Responsible Use Policy (RUP) is maintained on Cal Poly’s Information Security website and by reference is incorporated into this section of CAP.

240.5 Accessible Information Technology

240.5.1 Cal Poly complies with the CSU’s policy to make information technology resources and services accessible to all CSU students, faculty, staff and the general public regardless of disability.

240.5.2 This encompasses all technology products and services used to deliver academic programs and services, administrative, advancement and other services, student services, information technology services, and auxiliary programs and services.

240.5.3 Cal Poly is committed to demonstrating continuous improvement as part of a multi-year phased implementation consistent with the CSU Accessible Technology Initiative (ATI) approach which is driven by the following principles:

240.5.4 Technology accessibility is an institution-wide responsibility that requires commitment and involvement from leadership across the enterprise.

240.5.5 Technology access for individuals with disabilities must provide comparable functionality, affordability, and timeliness and should be delivered in as seamless a manner as possible.

240.5.6 The implementation of Universal Design principles should reduce the need for, and costs associated with, individual accommodations for inaccessible technology products.
Accessibility is an ongoing, shared responsibility that requires collaboration among faculty, staff, students and administration.

Under the executive sponsorship of the vice provost for Information Services/chief information officer, Cal Poly collaborates with campus constituents, the Chancellor’s Office and other CSU campuses to develop plans, identify resources, and establish standards and practices to achieve ATI goals:

1. Compliance with all applicable federal and state laws, regulations and CSU policies governing accessible technology;

2. Accessibility of instructional materials to allow for equally effective access for all faculty and students, as documented in campus guidelines and plans for accessible technology;

3. Accessibility of campus websites, web applications, and web content, as documented in campus guidelines and plans for accessible technology; and

4. Continued compliance with Section 508 of the Rehabilitation Act requirements for electronic and information technology procurement.

Cal Poly must acquire information technology products and services that comply with applicable federal accessibility standards when such products and services are available in the commercial marketplace. If a product or service is available and meets some, but not all of the relevant provisions, the product that best meets the standard must be procured. If compliance is unfeasible, then such exception shall be fully documented and approved by Cal Poly’s E&IT compliance officer.

Electronic and Information Technology (E&IT) Decisions

This policy is intended to assist campus units in making electronic and information technology decisions, to reduce both direct and indirect expenses, to better assess aggregate campus demand for technologies, to ensure access to and effective integration of technology on campus, to reduce risk, and to minimize the potential impact of adverse or unintended consequences to the University or its affiliated units and auxiliaries.

Acquisition, acceptance or development of E&IT products or services that materially affect Cal Poly’s users, assets, operations, or business continuity, or its ability to comply with existing policies, laws and related regulatory, legal or administrative practices, must conform to established campus standards, guidelines and practices for making technology decisions.
240.6.3 The standards and practices created to implement this policy shall establish the criteria for reviewing and making decisions, provide guidelines for required or recommended reviews and their conduct, and define the roles and responsibilities of those involved in the review process. The criteria shall consider potential impact and risk to the University; accessibility, security, policy and regulatory compliance issues; resource, operational and support issues; and integration and fit with established University priorities, infrastructure, services, systems and standards.

240.6.4 E&IT decisions must comply with all other applicable campus policies, including but not limited to contracts and procurement, conflict of interest, facilities etc.

240.6.5 This policy shall apply to all technology decisions that meet the campus criteria for review, regardless of who initiates the decision/request or the funding source. Any E&IT product or service may be subject to review based on substantive changes (e.g., technical, functional, operational) or its potential impact on campus users or the University.

240.6.6 The vice provost for Information Technology Services/chief information officer is responsible for application and enforcement of this policy. The VP/CIO or designee, in consultation with university procurement or other affected parties, is responsible for developing standards, guidelines and practices for implementing the policy.

240.7 Information Technology Advisory Committees

240.7.1 The vice provost/chief information officer consults with committees representing campus constituents regarding information technology plans, policies and priorities. Standing committees representing the campus leadership, faculty, administrators and students respectively are appointed annually by the President. Non-standing committees, advisory groups and working groups may be established as needed to advise on specific projects, initiatives, services or issues. Information about these committees will be maintained on the Office of the CIO website.

240.8 Information Authority for IT Records

240.8.1 The vice provost/chief information officer is the designated information authority for University data, communications and records that are the exclusive responsibility of Information Services. A list of applicable records is maintained in Cal Poly’s Business Continuity Plan.
The University generally prohibits access to electronic records and communications by anyone other than the designated owner of the source account or electronic resource, or the sender or recipient of a particular communication without prior consent from the applicable account owner, sender or recipient.

Information Technology Services will disclose records without such consent under the following conditions:

- In response to a valid subpoena, court order or other legal document to outside entities;
- When requested by an authorized University official for internal use;
- When fulfilling the legal, regulatory or other applicable duties of the University;
- When responding to an electronic or physical security issue or incident;
- In the event of an emergency or similar health or safety concerns; or
- To ensure the security, confidentiality, integrity and availability of Cal Poly information assets.

The Office of the CIO in consultation with University Legal Counsel and other University officials as appropriate to the circumstances will approve or deny requests to disclose records submitted in writing.

Requests must indicate what is being requested, the timeframe, the reason for the request, who requests receipt of the data, which condition above applies, and the intended use of the received data.

This provision applies to all user accounts and information resources, including those assigned to deceased, incapacitated or otherwise unreachable individuals.

Advertising and Sponsorship Acknowledgements on Cal Poly webpages

This policy applies to all Cal Poly webpages signified by the address ‘calpoly.edu’ or within the range of Internet and Intranet protocol addresses assigned to Cal Poly. Unless a specific exception has been granted, Cal Poly webpages residing outside the calpoly.edu domain or hosted on non-calpoly.edu servers must comply with the terms of this policy in order to be linked from the calpoly.edu home page. All University webpages and electronic publications, regardless of where they are hosted, must comply with applicable campus policies and standards.
In accordance with CSU and Cal Poly responsible use policies, any Cal Poly webpage or online publication created or maintained by or on behalf of the University must not be used for commercial, non-mission related purposes, personal financial gain, or any other use inconsistent with this policy.

Advertising space cannot be sold at any level of a Cal Poly webpage or online publication without the express approval of the President or designee. Advertising refers to any situation in which an individual or the University receives payment or in-kind gifts in exchange for a link or brand placement. While paid advertising is prohibited, links to commercial vendors may be made in the following specific situations:

1. Links to licensed software or other technologies on which a core function of the webpage is based (e.g., search engines, readers, viewers, etc.);
2. Links to a third party separately contracted to provide services to the University (e.g., Collegiate Licensing Company);
3. Links to an officially recognized Cal Poly presence on social media or other online sites;
4. Educational purposes (e.g., the text link provides information for educational or other mission-related purposes) and the University has received no consideration for incorporating that link; and
5. Where the President or designee has determined that special circumstances exist which warrant granting an exception to the general prohibition on advertising (e.g., Athletics website).

This policy does not prohibit web-based sale of non-commercial University products and materials related to Cal Poly’s educational, research and service mission. However, such sales must comply with campus information security policies and standards, such as the Payment Card Industry (PCI) requirements.

Sponsorship is non-University underwriting of a specific University event, publication or special activity (such as a scholarship fund drive) that represents the equivalent of a gift-in-kind or a gift of money insofar as the non-University sponsor provides or pays for promotion, materials, awards, and/or other items or services of value related to the specific event, publication or special activity. Sponsorship or acknowledgements of sponsorship are not advertising as defined in this policy.

Sponsorship recognition is permitted only if the following conditions are met:
240.9.6.1 The logo or name is displayed at a second level webpage or below;

240.9.6.2 The logo or name is not hyperlinked to the company webpage;

240.9.6.3 The display is consistent with University graphic standards or related requirements;

240.9.6.4 The logo or name of each sponsor is consistent in size, content and importance;

240.9.6.5 The context does not imply University endorsement of products or services offered by the sponsor;

240.9.6.6 Any descriptive text accompanying the logo must be value neutral (i.e., factual and objective, non-qualitative or comparative);

240.9.6.7 The recognition complies with all applicable institutional policies; and

240.9.6.8 Initial support was given by the sponsor with no expectation of a substantial return benefit.

240.9.7 The intent is to recognize corporate supporters of the University without commercializing the University and unit websites and online publications. Links to sponsors or other corporate recognition on a unit’s home page are not permitted except under special circumstances.

240.9.8 Exceptions may be granted on a case-by-case basis only, approved by the Office of the CIO in consultation with the appropriate campus authority.

240.10 Identity and Access Management

240.10.1 Accounts

Core accounts are provided for enterprise information resources and services, including but not limited to the Cal Poly Portal, email, calendar, CMS, PolyLearn, directory services, etc. Core accounts are provided to account owners in accordance with established eligibility requirements. Accounts are targeted for deletion when the owner no longer meets those eligibility requirements.

240.10.2 The following account types are provisioned by Information Technology Services (ITS):

240.10.2.1 Individual accounts for each eligible student, faculty, staff and emeritus employee;
Organizational accounts for each unique Cal Poly entity or service, standing committee, chartered student club, affiliated center or institute, and instructional related activity;

Auxiliary accounts, both individual and organizational, on an incremental cost-recovery basis; and

Affiliated accounts for individuals not covered above who require access to University resources, either in direct support of the instructional mission, or in support of administrative and institutional needs of the University. Affiliated user accounts must be sponsored by a recognized University organization, approved by an authorized administrator, and renewed annually.

Unless eligible through another affiliation, Cal Poly alumni are not eligible to maintain their accounts once they graduate. Alumni are eligible for email forwarding and other services through the Cal Poly Alumni Association.

Cases where eligibility is disputed or unclear will be escalated to the Office of the CIO for review and resolution, in consultation with the appropriate offices of record.

Access to information resources and services are tied to the role or relationship that the individual has with the university. ITS works with the offices of record, sponsors, and service providers to adjust privileges when the individual's role or relationship changes. ITS will expedite the account expiration process, up to and including the immediate revocation of all privileges, with written authorization from the appropriate information authority, e.g., Academic Personnel for faculty, Human Resources for staff, vice president for Student Affairs for students.

Authentication Services

To protect campus resources from unauthorized use, Cal Poly requires all users to authenticate their individual identity and eligibility to use those resources. Unique identification and authentication credentials shall be assigned to each user for this purpose, i.e., Cal Poly username and password. The person to whom the credentials are assigned is the only authorized user of those credentials.

ITS is responsible for the design, implementation and operation of Cal Poly’s centralized authentication services, including the assignment of Cal Poly username and password to users of enterprise resources. ITS shall assign, activate, de-activate, revoke or otherwise modify a user’s credentials based upon the user’s verified identity and current university affiliations as reflected in official University record systems. Owners and administrators of University applications
and services shall utilize the University’s standard authentication service and credentials to validate the identity of all users of the application or service unless otherwise exempted.

240.12 Cal Poly Username

240.12.1 Upon creation, each account is assigned a unique, permanent electronic identifier (Cal Poly username) and a temporary password. Cal Poly usernames are created and assigned following a standard naming convention to ensure their uniqueness and suitability as identifiers. Account owners may not specify or personally choose their Cal Poly usernames. Individuals may not possess more than one concurrently active Cal Poly username.

240.12.2 Under normal circumstances, ITS will replace the automatically assigned username with a different username only if the replacement complies with the University’s standard naming convenience and one of the following conditions exists:

240.12.2.1 The account owner legally changes their name, registers the change in the official University database, and requests a replacement username;

240.12.2.2 The existing Cal Poly username represents a credible danger to the health or safety of the account owner; or

240.12.2.3 The Cal Poly username produced by the algorithm results in a combination of characters considered offensive or inappropriate by either the account owner or the University.

240.13 Cal Poly Password

240.13.1 To avoid unauthorized access to IT resources, holders of Cal Poly electronic identifiers must follow established rules for creating and using, and for reporting the suspected compromise of the complex passwords that correspond to a Cal Poly electronic identifier.

240.13.2 The Cal Poly password must be changed immediately upon issuance, when an account is compromised or suspected to be compromised, and at least annually thereafter. Account owners must affirm their knowledge and understanding of their responsibilities relative to information security and the appropriate use of
information resources each time they change it. The Cal Poly password must never be shared with anyone else or used for any non-University service.

240.14 Electronic Mail and Messaging

240.14.1 University electronic mail and messaging is to be used to enhance teaching, learning, scholarly research, to support academic experiences, and to facilitate the effective business and administrative processes of the University.

240.14.2 These policies are applicable to all users (departments, organizations, individuals) of any Cal Poly email or messaging system.

240.14.3 Users are expected to comply with all applicable laws and University policies and standards affecting the use of electronic mail and messaging and related systems, including but not limited to Cal Poly’s Information Security Program, Responsible Use Policy, Confidentiality-Security Agreements, and Use and Release of Student Information Policy.

240.14.4 Consistent with CSU/campus data classification and handling standards, electronic mail and messaging should be avoided as a means of communicating confidential or sensitive material inasmuch as messages can be intercepted, copied, read, forged, destroyed or misused by others for mischievous purposes.

240.14.5 The University reserves the right to:

240.14.5.1 Limit the size of individual mail messages being transmitted through University resources;

240.14.5.2 Send email to its own users;

240.14.5.3 Retain copies of messages on system backups for periods of time and locations unknown to users; and

240.14.5.4 Monitor the contents of files or messages only when necessary to preserve either system integrity or continued email delivery or in support of an official University investigation. Any other monitoring by system administrators is prohibited.

240.14.6 Email and electronic messages, whether or not created or stored on University equipment, may constitute a University record subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. This includes email-related data stored in electronic form on any device, regardless of ownership. Copies of e-mail must be provided in response to a public record request or legally issued subpoena, subject to very limited exceptions, as with all other documents created and retained at the University.
240.14.7 Prohibited activities include but are not limited to:

240.14.7.1 Altering electronic communications to hide one's identity or to impersonate another individual which is considered misrepresentation and/or forgery;

240.14.7.2 Sending unsolicited commercial advertisements or other types of solicitations (e.g., spam, phishing emails);

240.14.7.3 Sending a large volume of unsolicited mail in an attempt to disrupt another entity;

240.14.7.4 Taking any action that may have the effect of seriously degrading system performance;

240.14.7.5 Using electronic communications with the intent to annoy, harass and/or physically threaten other individuals;

240.14.7.6 Using state resources, including email, for anyone's private financial or political gain, including promoting off-campus for-profit and non-profit sales and services; and

240.14.7.7 Operating an unauthorized email reflector that automatically forwards messages to multiple recipients triggered by the content or headers of the mail message being forwarded. [Suggested revision: “Operating an unauthorized email reflector that automatically forwards messages to members on a distribution list.”]

240.14.8 Large group mailings are permitted only if sent via authorized distribution methods to reduce system loads. Examples include class lists, college and department lists (e.g., faculty and staff rosters), committees, student clubs, other official University organizations, and specific discussion/topic groups.

240.14.9 Distribution lists are to be used only for the purpose for which they were created. For example, class lists are for use by classes in class discussions and dissemination of information within the context of the specified class. Student club lists are for disseminating official club information. All other lists are for use by specific units or members to disseminate or share information. Use of such lists by non-authorized personnel violates this policy.

240.14.10 University lists may not be used to broadcast unofficial and/or unauthorized messages. Lists established to broadcast information may not be used without the express permission of the owner of the list.

240.15 Broadcast Electronic Message Policy
Broadcast messaging is unsolicited email, texts or any electronic communication sent quickly in large quantities to facilitate communication of urgent, time-critical or other essential University information to the entire campus community or segments therein. Broadcast messaging is considered an appropriate form for communication under the following circumstances:

240.15.1.1 Provides essential information for the operation or execution of University business;

240.15.1.2 Notifies the University community of significant events or changes in governance, policy and practice;

240.15.1.3 Alerts the University community to situations affecting health and safety; and

240.15.1.4 Communicates information deemed essential by a University authority and carrying the signature of that authority.

240.15.2 Broadcast messages require prior written approval of the appropriate University official. The following university officials (or designees) must approve broadcast messages to the specified group(s):

240.15.2.1 Faculty (State) and non-faculty instructors – provost;

240.15.2.2 Students – vice president for student affairs;

240.15.2.3 Staff (State) – vice president for administration and finance;

240.15.2.4 Other employee groups (CPC, ASI, Emeritus) – vice president for administration and finance; and

240.15.2.5 Entire campus or any one or combination of the above – President or provost.

240.15.3 To facilitate broadcast messages, Information Technology Services (ITS) maintains distribution lists of all current students, faculty and staff, non-faculty instructors, emeritus and auxiliary employees. Messages being broadcast to one or more of these groups must be approved by the Office of the CIO, use an approved broadcast method, and meet the following criteria:

240.15.3.1 Is such that the timeliness and nature of the information or event cannot be communicated effectively by other means;

240.15.3.2 Targets an appropriate audience who will benefit significantly from the communication;
240.15.3.3 Complies with applicable University policies on use of State resources; and

240.15.3.4 Prevents significant inconvenience to the targeted audience if the information is not shared.

240.15.4 Units within the University, such as a college or department, may initiate broadcast messages containing official University business to their own constituent groups (e.g., all students or employees within that unit) without seeking University approval, but should still observe these criteria. Such mailings should be consistent with the policy, standards, guidelines and procedures detailed in the policy Electronic Mail as an Official Means of Communication to Students. (CAP 240.16)

240.15.5 The University reserves the right to perform broadcast mailings which are related to emergencies and University physical plant conditions or activities for which urgent notice is required and that will potentially affect most of the recipients.

240.15.6 A limited number of campus entities have been pre-approved to send specific types of broadcast mailings based on operational needs. Misuse may result in the revoking of authorization.

240.15.7 The University reserves the right to track and analyze the effective of its electronic communications by collecting aggregate statistics on readership and technology use, including role-based variances. Cal Poly will not monitor individual responses unless required to do so by law or for other valid business requirements, and only with prior approval of the President or Provost.

240.15.8 Inappropriate broadcast messaging may be considered an abuse of University information technology resources. Inappropriate broadcast message topics include, but are not limited to:

240.15.8.1 Any message whose content is not relevant to Cal Poly’s mission of teaching, research and public service;

240.15.8.2 Any message that violates existing policies or laws;

240.15.8.3 Announcement of events except where it impacts the entire campus community;

240.15.8.4 Any message pertaining to individual student club or group activities;

240.15.8.5 Any message pertaining to individual student, group or class projects;

240.15.8.6 Any commercial mailing;
240.15.8.7 Any solicitations;
240.15.8.8 Personal messages; or
240.15.8.9 Political advocacy

240.16 Electronic Messaging as an Official Means of Communication to Students

240.16.1 Electronic messaging shall be considered an appropriate, cost-effective, convenient and timely means to transmit official campus communications to students. An official communication occurs when an individual or campus entity sends electronic mail or other message pertinent to conducting University business for academic or administrative purposes, including notification of University-related actions.

240.16.2 Official email communications will be sent to a student’s University-assigned email address (username@calpoly.edu). Other methods may be used when authorized by the individual (e.g., text messaging) or approved by the University (e.g., portal notifications) for this purpose.

240.16.3 Electronic messaging may be the sole method for notification. However, additional or other methods of communication will be utilized if appropriate or required by law or other contractual obligations (e.g., notification of disciplinary and legal actions).

240.16.4 Electronic messages sent as official campus communications are expected to comply with applicable laws and campus policies, including those referenced in this policy, and are subject to the same public records, privacy and records retention requirements and policies as other official campus communications.

240.17 PolyCard Identification Card

240.17.1 Information Technology Services is responsible for managing the production and distribution of Cal Poly’s official identification card known as PolyCard.

240.17.2 ITS will issue one active PolyCard to each eligible user for use during their tenure at Cal Poly based upon the individual's primary affiliation with the University. The name appearing on the PolyCard will be the cardholder’s official (primary) name on record with the University.

240.17.3 PolyCards are issued to currently active students, faculty, staff and emeriti who are provisioned in Cal Poly’s data warehouse and identity management system. All other user types, including affiliated persons and applicants, are ineligible to receive a PolyCard.
240.17.4 Exceptions may be granted on a case-by-case basis only, approved by the Office of the CIO in consultation with the appropriate campus authority.

240.17.5 PolyCards are the property of Cal Poly, not the individual cardholder, and the University governs all uses of the PolyCard. The PolyCard itself is non-transferable. It must be presented or surrendered to campus authorities, including ITS, upon demand. PolyCards become invalid upon termination of affiliation with the University.

240.17.6 Unauthorized use, sharing, alteration or duplication for fraudulent purposes will result in immediate confiscation of the card and may result in disciplinary or legal action.

240.17.7 Lost or stolen cards will be deactivated upon notification and will no longer function electronically. Found cards must be returned to the ITS service desk and will be destroyed. Damaged or mutilated cards must be brought to the ITS service desk and surrendered at the time of replacement. An additional charge will be assessed to all users for each replacement card except for replacement of PolyCards that are faded or rendered unusable due to normal wear and tear.

240.17.8 Use of the PolyCard for campus services must be reviewed and approved by ITS and other appropriate campus authorities using established procedures. Unauthorized uses violate this policy. Approved uses of the PolyCard must conform to all applicable laws and policies. This includes but is not limited to Cal Poly’s Information Security Program, Responsible Use Policy, Confidentiality-Security Agreements, and Use and Release of Student Information Policy.

240.17.9 Use of PolyCard photographs will be subject to applicable policies and laws.

240.17.10 In accordance with the Family Education Rights and Privacy Act (FERPA), a student’s ID card photograph is part of his or her educational record. As directory information, it can be released to campus officials for educationally related and University purposes. The University will not release a student photograph outside the institution, unless permitted or required by law.

240.17.11 State and auxiliary employee and other non-student photographs are protected by the Information Practices Act and will not be released unless permitted or required by law.

240.17.12 Requests to release photos must be in writing and approved by the Office of the CIO. Except in an emergency where health and safety is an issue, a photographic release form signed by the affected individual must be on file prior to the release of the photo.
Data collected and stored electronically in conjunction with the uses of the PolyCard is subject to the same restrictions and guidelines noted above. While the PolyCard office does not track individual card use, it may provide general demographic data to campus service providers on the use of their services.

University Networks and Airwaves Policy

Information Technology Services is responsible for the University's data, video and voice communications network. This includes designing, deploying, documenting, monitoring, maintaining, supporting and troubleshooting the physical data, video and voice networks of the university, as well as the management of the Internet Protocol (IP) address spaces (including public and private addresses) assigned to Cal Poly.

This policy applies to all users of Cal Poly information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

Neither individuals nor units are permitted to independently deploy network devices that extend the University network, or secure or isolate parts of the University network, except as approved by Information Technology Services.

If not deployed and configured correctly, network devices such as hubs, bridges, switches, routers, firewalls, wireless access points (WAPs), network address translators (NATs), remote access servers (RAS), and virtual private network (VPN) servers can cause service interruptions and difficulties. In addition, if not properly secured, these devices can give unauthorized users access to the University network. The installation and configuration of these devices must therefore be managed and coordinated by ITS.

Information Technology Services recognizes the increased use and availability of various wireless technologies at Cal Poly. These wireless systems present new and serious security challenges that must be addressed in order to provide the utmost accountability and reliability in network use.

ITS is responsible to the Cal Poly community and its constituents for providing a communication network that is accessible, reliable, secure and well performing. To ensure this level of service, the airwaves supporting campus wireless technologies must be managed in a coordinated manner. ITS manages this airspace for the campus and will act as the asset steward, consistent with the managed utility design in place throughout the campus. Therefore, any Cal Poly college, department, unit or individual who wishes to utilize wireless technology
on campus must follow ITS stated policies, standard protocols, practices and procedures.

240.19 Domain Name Registration and Usage

240.19.1 Domain names are electronic addresses used to find specific destinations and services on the Internet. Domain names can be an important part of a unit’s identity and public outreach efforts and therefore have an impact on how the University as a whole is perceived.

240.19.2 To ensure a coherent process for assigning domain names, Cal Poly maintains a record of its domain name assets and centrally manages registration of all University-related domain names. Information Technology Services is the official institutional contact and registrant of domain names on behalf of Cal Poly, including those outside the calpoly.edu domain. This policy ensures protection and continued use of Cal Poly domain names, compliance with applicable policies and laws, and prevents inappropriate and unauthorized uses.

240.19.3 This policy applies to any state entity, affiliate or individual registering a domain name for University-related purposes; any domain name pointing to a University-owned computer; any University-related activity or service requiring a domain name regardless of where it is hosted or how it is funded.

240.19.4 This includes: University divisions, colleges, departments, auxiliaries, instructionally related activities, sponsored programs, institutes and centers, student clubs and organizations, and services associated with Cal Poly domain names that are contractually delegated to or operated by non-University entities.

240.19.5 The principal domain name for Cal Poly is “calpoly.edu”. All machines connected to the Cal Poly network must be registered in the Cal Poly Domain Name System (DNS) and all hosts on the Cal Poly network must be registered inside the calpoly.edu domain. All domain names must resolve to a Cal Poly IP address unless a specific exception has been granted. Any Cal Poly IP address must formally resolve to a registered name in the calpoly.edu domain.

240.19.6 Websites and services provided by members of the Cal Poly community as part of their official function or as part of Cal Poly’s mission must be registered and hosted within the calpoly.edu domain. This includes personal websites residing on University servers.

240.19.7 Exceptions will be granted by the Office of the CIO if a non-calpoly.edu domain name is appropriate and necessary to convey the identity, function or nature of an established entity, activity or service, or to prevent a non-calpoly.edu domain
240.17.13  Data collected and stored electronically in conjunction with the uses of the PolyCard is subject to the same restrictions and guidelines noted above. While the PolyCard office does not track individual card use, it may provide general demographic data to campus service providers on the use of their services.

240.18  University Networks and Airwaves Policy

240.18.1  Information Technology Services is responsible for the University's data, video and voice communications network. This includes designing, deploying, documenting, monitoring, maintaining, supporting and troubleshooting the physical data, video and voice networks of the university, as well as the management of the Internet Protocol (IP) address spaces (including public and private addresses) assigned to Cal Poly.

240.18.2  This policy applies to all users of Cal Poly information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

240.18.3  Neither individuals nor units are permitted to independently deploy network devices that extend the University network, or secure or isolate parts of the University network, except as approved by Information Technology Services.

240.18.4  If not deployed and configured correctly, network devices such as hubs, bridges, switches, routers, firewalls, wireless access points (WAPs), network address translators (NATs), remote access servers (RAS), and virtual private network (VPN) servers can cause service interruptions and difficulties. In addition, if not properly secured, these devices can give unauthorized users access to the University network. The installation and configuration of these devices must therefore be managed and coordinated by ITS.

240.18.5  Information Technology Services recognizes the increased use and availability of various wireless technologies at Cal Poly. These wireless systems present new and serious security challenges that must be addressed in order to provide the utmost accountability and reliability in network use.

240.18.6  ITS is responsible to the Cal Poly community and its constituents for providing a communication network that is accessible, reliable, secure and well performing. To ensure this level of service, the airwaves supporting campus wireless technologies must be managed in a coordinated manner. ITS manages this airspace for the campus and will act as the asset steward, consistent with the managed utility design in place throughout the campus. Therefore, any Cal Poly college, department, unit or individual who wishes to utilize wireless technology
on campus must follow ITS stated policies, standard protocols, practices and procedures.

240.19 Domain Name Registration and Usage

Domain names are electronic addresses used to find specific destinations and services on the Internet. Domain names can be an important part of a unit’s identity and public outreach efforts and therefore have an impact on how the University as a whole is perceived.

To ensure a coherent process for assigning domain names, Cal Poly maintains a record of its domain name assets and centrally manages registration of all University-related domain names. Information Technology Services is the official institutional contact and registrant of domain names on behalf of Cal Poly, including those outside the calpoly.edu domain. This policy ensures protection and continued use of Cal Poly domain names, compliance with applicable policies and laws, and prevents inappropriate and unauthorized uses.

This policy applies to any state entity, affiliate or individual registering a domain name for University-related purposes; any domain name pointing to a University-owned computer; any University-related activity or service requiring a domain name regardless of where it is hosted or how it is funded.

This includes: University divisions, colleges, departments, auxiliaries, instructionally related activities, sponsored programs, institutes and centers, student clubs and organizations, and services associated with Cal Poly domain names that are contractually delegated to or operated by non-University entities.

The principal domain name for Cal Poly is “calpoly.edu”. All machines connected to the Cal Poly network must be registered in the Cal Poly Domain Name System (DNS) and all hosts on the Cal Poly network must be registered inside the calpoly.edu domain. All domain names must resolve to a Cal Poly IP address unless a specific exception has been granted. Any Cal Poly IP address must formally resolve to a registered name in the calpoly.edu domain.

Websites and services provided by members of the Cal Poly community as part of their official function or as part of Cal Poly’s mission must be registered and hosted within the calpoly.edu domain. This includes personal websites residing on University servers.

Exceptions will be granted by the Office of the CIO if a non-calpoly.edu domain name is appropriate and necessary to convey the identity, function or nature of an established entity, activity or service, or to prevent a non-calpoly.edu domain
name from being misappropriated. This includes Web sites and services delegated to, maintained or operated by non-University entities on behalf of the University. The University entity requesting the non-calpoly.edu domain name is responsible for any related costs. All non-calpoly.edu domain name requests are subject to availability.

240.19.8 Use of the term “calpoly” is protected by state law. University approval is required prior to registering a non-calpoly.edu domain name that contains the term “calpoly” or Cal Poly logos, seals or trademarks.

240.19.9 Individuals and organizational units are not authorized to register Internet domain names on behalf of Cal Poly or their respective units. Members of the Cal Poly community are not permitted to register a non calpoly.edu domain name that resolves (points) to a computer or service on campus.

240.19.10 Non-calpoly.edu domain names registered without Office of the CIO approval must be transferred to ITS control as soon as possible. Any resulting costs will be borne by the responsible University entity.

240.19.10.1 Domain names associated with student clubs and organizations will be reviewed and approved by the Office of the CIO through the annual club chartering process.

240.20 Telephone Service and Usage

240.20.1 Information Technology Services is budgeted to provide each full-time faculty (or full-time equivalent), each full-time state staff member and each state department as determined by the department head with a telephone line, a digital telephone set with standard features and a voice mailbox. Additional phones and phone services provided to non-State funded entities will be charged back.

240.20.2 University-owned cellular telephones (i.e., telephones connected to a commercial cellular telephone service) may be assigned to campus individuals or departments for whom the nature of their work requires wide mobility and who have a more explicit need to have access to or to be readily accessible by others. The justification for cellular telephone service should have a clear connection to the employer’s job responsibilities. ITS will assign University-owned cellular phones based on certification of the need by the appropriate administrator.

240.20.3 All costs associated with University-owned cellular phones will be borne by the department that requests cellular service. These costs include, but are not limited to, equipment and accessories purchase, service activation, monthly service and feature charges, usage charges, insurance, taxes and surcharges.
240.20.4 Information Technology Services is responsible for initiating University cellular phone transactions (i.e., phone purchases, service activations/terminations, etc.) using established contracts with commercial vendors.

240.20.5 Faculty and staff may not transfer existing personal (non-Cal Poly) cellular services to Cal Poly cellular service accounts. New service requests require a new contract with the vendor and thus, a new wireless number will be generated. Existing Cal Poly, department-sponsored cellular services may be transferred between service accounts.

240.20.6 Cellular phones purchased on the Cal Poly government account with state funds are considered state property and must be returned to the University upon termination of employment.

240.20.7 Unless specifically authorized by the department with compelling use for this technology, University-provided cellular telephones may not be issued to student workers.

240.20.8 The individual assigned to the University-provided telephone is responsible for taking appropriate steps to secure the phone and notifying the ITS service desk if the phone is lost, stolen or misplaced. The department is responsible for covering replacement costs.

240.20.9 Use of campus telephones/facsimile machines and University-owned cellular telephone and airtime service is intended for official University business only and must comply with applicable laws and University policies, including information security policies and standards.

240.20.10 Government Code Section 8314 prohibits state employees from using public resources for "a campaign activity or personal or other purposes which are not authorized by law." However, "incidental and minimal" personal use is permitted, provided such use does not consume excessive public resources, interfere with the performance of one's job or other University responsibilities, and conforms to applicable laws, rules, policies, contracts and licenses.

240.20.11 As a general rule, personal calls and faxes should not be made from or billed to the University. However, if an employee uses a campus telephone or facsimile machine to place personal calls or send personal faxes, then:

240.20.11.1 The number and length should be kept to a minimum;

240.20.11.2 Such calls must not interfere with University business; and
240.20.11.3 The employee is responsible for reimbursing any direct costs incurred by the University.

240.20.12 Costs for all personal calls (emergency, home, family, etc.) made from or received on the University-provided cellular telephone must be reimbursed on a monthly basis. Reimbursements for personal calls will not exceed the carrier’s charges to the University.

240.20.13 Unless authorized in advance by the appropriate administrator, the University will not reimburse individuals for costs associated with non-University owned or provided cellular phones used for Cal Poly business. This includes, but is not limited to, monthly service and feature charges, usage charges, taxes, fees and surcharges.

References for CAP 240:

1. Date approved by the President: To be determined.
2. Effective Date: To be determined.
3. Responsible Department/Office: Information Technology Services
4. Revision History: Use when applicable.
5. Related University Policies, Procedures, Manuals and/or Documents:
   a. Cal Poly Information Security Program (full text)
   b. Cal Poly Responsible Use Policy (full text) and related appendices -
      http://security.calpoly.edu/content/policies/rup/index
   c. Cal Poly Information Security Standards - data classification and handling, managing computer accounts, incident response, passwords, email retention, etc.
      http://security.calpoly.edu/content/policies/standard_list
   d. Cal Poly Information Technology/Security Exception Request Process -
      http://www.security.calpoly.edu/content/exception-process
   e. Confidentiality-Security Agreements
      http://www.security.calpoly.edu/content/policies/confidentiality_security_agreements
   f. Cal Poly Copyright Infringement Practices
      http://www.security.calpoly.edu/content/copyright/heoa
   g. Cal Poly Guidelines for Use of Electronic Recording Devices
      http://www.security.calpoly.edu/content/policies/recording_devices
   h. Cal Poly Business Continuity Planning Website
      http://afd.calpoly.edu/acs/buscontinuity.asp
   i. Cal Poly Credit Card Acceptance Website (PCI Compliance Practices)
      https://afd.calpoly.edu/fiscalservices/pci/
   j. Cal Poly Office of Student Rights and Responsibilities: Standards for Student Conduct
      http://www.osrr.calpoly.edu/
240.20.11.3 The employee is responsible for reimbursing any direct costs incurred by the University.

240.20.12 Costs for all personal calls (emergency, home, family, etc.) made from or received on the University-provided cellular telephone must be reimbursed on a monthly basis. Reimbursements for personal calls will not exceed the carrier’s charges to the University.

240.20.13 Unless authorized in advance by the appropriate administrator, the University will not reimburse individuals for costs associated with non-University owned or provided cellular phones used for Cal Poly business. This includes, but is not limited to, monthly service and feature charges, usage charges, taxes, fees and surcharges.

**References for CAP 240:**

1. Date approved by the President: To be determined.
2. Effective Date: To be determined.
3. Responsible Department/Office: Information Technology Services
4. Revision History: Use when applicable.
5. Related University Policies, Procedures, Manuals and/or Documents:
   a. Cal Poly Information Security Program (full text)
   b. Cal Poly Responsible Use Policy (full text) and related appendices -
      http://security.calpoly.edu/content/policies/rup/index
   c. Cal Poly Information Security Standards - data classification and handling, managing computer accounts, incident response, passwords, email retention, etc.
      http://security.calpoly.edu/content/policies/standard_list
   d. Cal Poly Information Technology/Security Exception Request Process -
      http://www.security.calpoly.edu/content/exception-process
   e. Confidentiality-Security Agreements
      http://www.security.calpoly.edu/content/policies/confidentiality_security_agreements
   f. Cal Poly Copyright Infringement Practices
      http://www.security.calpoly.edu/content/copyright/heoa
   g. Cal Poly Guidelines for Use of Electronic Recording Devices
      http://www.security.calpoly.edu/content/policies/recording_devices
   h. Cal Poly Business Continuity Planning Website
      http://afd.calpoly.edu/acs/buscontinuity.asp
   i. Cal Poly Credit Card Acceptance Website (PCI Compliance Practices)
      https://afd.calpoly.edu/fiscalservices/pci/
   j. Cal Poly Office of Student Rights and Responsibilities: Standards for Student Conduct
      http://www.osrr.calpoly.edu/
k. Cal Poly Academic Policy on Cheating and Plagiarism
   http://www.academicprograms.calpoly.edu/content/academicpolicies/Cheating
m. Cal Poly Office of the Registrar FERPA Website
   http://www.registrar.calpoly.edu/content/stu_info/ferpa
n. Cal Poly/CSU Academic Senate Resolutions on Accessibility
   http://www.accessibility.calpoly.edu/content/policies
o. Cal Poly Presidential Directives on Accessible Technology
   http://www.accessibility.calpoly.edu/content/news/index
p. Cal Poly Accessible Information Technology Website
   http://www.accessibility.calpoly.edu/content/it
q. Cal Poly Web Accessibility Compliance Guide
   http://www.warc.calpoly.edu/accessibility/compliance_process_guide.html
r. Cal Poly Electronic & Information Technology Decisions: Standards and Practices
s. Cal Poly Technology Purchases Website
   http://afd.calpoly.edu/cprm/computers.asp?pid=2
t. Cal Poly Fiscal Services Cell Phone policy and related forms
   https://afd.calpoly.edu/fiscalservices/forms.asp
u. Cal Poly Trademark Licensing Website https://afd.calpoly.edu/tm_licensing/
v. Cal Poly Graphic Standards and Campus Style Guide
   http://www.marketingcomm.calpoly.edu/
w. Cal Poly Email Policies, Standards, Guidelines and Practices
   http://servicedesk.calpoly.edu/content/email_calendar/policy/index
x. Cal Poly Password Manager FAQs and Password Requirements
   http://servicedesk.calpoly.edu/content/computing_support/faq/password
y. Cal Poly Accounts
   http://www.servicedesk.calpoly.edu/content/accounts_passwords/index
z. PolyCard Services and Procedures http://polycard.calpoly.edu/

aa. Cal Poly Network Services, Policies/Procedures and Forms
   http://www.netadmin.calpoly.edu/

bb. CAP 140: Free Expression, Sponsorship, Commercialism, and Use of Buildings and Grounds
cc. CAP 145: Policy on Use of University Names and Marks
dd. CAP 740.1.4: Placement of Advertisements
ee. CAP 382: Requests for Public Records
ff. CAP 231.2: Policy of the Use and Release of Student Information
gg. CSU Information Security Policy and related standards, including responsible use, electronic and digital signatures, etc.
   http://www.calstate.edu/icsuam/documents/Section8000.pdf
hh. CSU Executive Order 1014 – Business Continuity Program
   http://www.calstate.edu/eo/EO-1014.html
jj. CSU Executive Order 926 – The CSU Board of Trustees Policy on Disability Support and Accommodations http://www.calstate.edu/EO/EO-926.html
kk. CSU Coded Memorandum AA-2013-03, Accessible Technology Initiative http://www.calstate.edu/AcadAff/codedmemos/AA-2013-03.html
mm. CSU Office of General Counsel Manuals on Legal Issues (e.g., copyright, etc.) http://www.calstate.edu/gc/OGC_Manuals_on_Legal_Issues.shtml
nn. Ownership and Appropriate Use of the CSU Name http://www.calstate.edu/gc/csujj
oo. CSU Identity and Access Management Initiative http://its.calstate.edu/iam/

6. Laws, Regulations and/or Codes of practice referred to herein or related to this policy:
   a. California Code of Regulations, Title V, Sections 42396 - 42396.5 http://tiny.cc/1rwn4x
   b. Title 5, Article 2, Section 41301 – Student Discipline – Misuse of computer facilities or resources http://tiny.cc/7xwn4x
   e. California Senate Bill 1386 (SB 1386) https://it.ucsf.edu/policies/california-senate-bill-1386-sb1386
   g. California Government Code Section 11135 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=11001-12000&file=11135-11139.7
   h. California State Penal Code Section 502 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9
   i. California State Penal Code Section 653m http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=639-653.2
   j. California Education Code 67302 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=edc&group=67001-68000&file=67300-67302.5
   k. California Education Code Section 89005.5 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=edc&group=88001-89000&file=89000-89011
   l. Fair and Accurate Credit Transactions Act (FACTA) https://www.privacyrights.org/fs/fs6a-facta.htm
n. Health Information Portability and Accountability Act of 1996 (HIPPA)  
   http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx
o. Gramm-Leach-Bliley Act (GLBA)  
q. Payment Card Industry Data Security Standard (PCI DSS)  
   https://www.pcisecuritystandards.org/merchants/how_to_be_compliant.php
r. Digital Millennium Copyright Act of 1998  
t. Americans with Disabilities Act (ADA) http://www.dol.gov/dol/topic/disability/ada.htm
u. Section 504 of the Rehabilitation Act of 1973  
   http://www.hhs.gov/ocr/civilrights/resources/factsheets/504.pdf
v. Section 508 Amendment to the Rehabilitation Act of 1973  
   https://www.section508.gov/content/learn/laws-and-policies
w. Section 508 Standards  
x. Internet Corporation of Assigned Names and Numbers (ICANN) -  
   https://www.icann.org/
k. Cal Poly Academic Policy on Cheating and Plagiarism
   http://www.academicprograms.calpoly.edu/content/academicpolicies/Cheating
m. Cal Poly Office of the Registrar FERPA Website
   http://www.registrar.calpoly.edu/content/stu_info/ferpa
n. Cal Poly/CSU Academic Senate Resolutions on Accessibility
   http://www.accessibility.calpoly.edu/content/policies
o. Cal Poly Presidential Directives on Accessible Technology
   http://www.accessibility.calpoly.edu/content/news/index
p. Cal Poly Accessible Information Technology Website
   http://www.accessibility.calpoly.edu/content/it
q. Cal Poly Web Accessibility Compliance Guide
   http://www.warc.calpoly.edu/accessibility/compliance_process_guide.html
r. Cal Poly Electronic & Information Technology Decisions: Standards and Practices
s. Cal Poly Technology Purchases Website
   http://afd.calpoly.edu/cprm/computers.asp?pid=2
t. Cal Poly Fiscal Services Cell Phone policy and related forms
   https://afd.calpoly.edu/fiscalservices/forms.asp
u. Cal Poly Trademark Licensing Website https://afd.calpoly.edu(tm_licensing)/
v. Cal Poly Graphic Standards and Campus Style Guide
   http://www.marketingcomm.calpoly.edu/
w. Cal Poly Email Policies, Standards, Guidelines and Practices
   http://servicedesk.calpoly.edu/content/email_calendar/policy/index
x. Cal Poly Password Manager FAQs and Password Requirements
   http://servicedesk.calpoly.edu/content/computing_support/faq/password
y. Cal Poly Accounts
   http://www.servicedesk.calpoly.edu/content/accounts_passwords/index
z. PolyCard Services and Procedures http://polycard.calpoly.edu/
aa. Cal Poly Network Services, Policies/Procedures and Forms
   http://www.netadmin.calpoly.edu/
bb. CAP 140: Free Expression, Sponsorship, Commercialism, and Use of Buildings and
   Grounds
cc. CAP 145: Policy on Use of University Names and Marks
dd. CAP 740.1.4: Placement of Advertisements
ee. CAP 382: Requests for Public Records
ff. CAP 231.2: Policy of the Use and Release of Student Information
gg. CSU Information Security Policy and related standards, including responsible use,
   electronic and digital signatures, etc.
   http://www.calstate.edu/icsuam/documents/Section8000.pdf
6. Laws, Regulations and/or Codes of practice referred to herein or related to this policy:
   a. California Code of Regulations, Title V, Sections 42396 - 42396.5 http://tiny.cc/1rwn4x
   b. Title 5, Article 2, Section 41301 – Student Discipline – Misuse of computer facilities or resources http://tiny.cc/7xwn4x
   e. California Senate Bill 1386 (SB 1386) https://it.ucsf.edu/policies/california-senate-bill-1386-sb1386
   g. California Government Code Section 11135 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=11001-12000&file=11135-11139.7
   h. California State Penal Code Section 502 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9
   i. California State Penal Code Section 653m http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=639-653.2
   j. California Education Code 67302 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=edc&group=67001-68000&file=67300-67302.5
   k. California Education Code Section 89005.5 http://www.leginfo.ca.gov/cgi-bin/displaycode?section=edc&group=88001-89000&file=89000-89011
   l. Fair and Accurate Credit Transactions Act (FACTA) https://www.privacyrights.org/fs/fs6a-facta.htm
n. Health Information Portability and Accountability Act of 1996 (HIPPA) 
   http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx
o. Gramm-Leach-Bliley Act (GLBA) 
p. Information Practices Act of 1977 (IPA) http://chancellor.berkeley.edu/services/public-
   records/about-information-practices-act-ipa
q. Payment Card Industry Data Security Standard (PCI DSS) 
   https://www.pcisecuritystandards.org/merchants/how_to_be_compliant.php
r. Digital Millennium Copyright Act of 1998 
t. Americans with Disabilities Act (ADA) http://www.dol.gov/dol/topic/disability/ada.htm
u. Section 504 of the Rehabilitation Act of 1973 
   http://www.hhs.gov/ocr/civilrights/resources/factsheets/504.pdf
v. Section 508 Amendment to the Rehabilitation Act of 1973 
   https://www.section508.gov/content/learn/laws-and-policies
w. Section 508 Standards 
   http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-
   section-508-standards
x. Internet Corporation of Assigned Names and Numbers (ICANN) - 
   https://www.icann.org/