Term/Acronym	Definition
Amendment	Contract amendments are created when changes are required on an approved (Executed) contract and the changes will affect the terms and conditions (duration, language/scope, and/or cost) of the contract.
Approval to Purchase (AtP)	**For President's Office (UMPO) ONLY** – To maintain budget controls and approval processes, the Approval to Purchase (AtP) form was created as the entry point for initiating or amending contracts for services and requisitions to purchase goods. The AtP form requires basic information about the need for the purchase, along with a justification statement as to the criticality of this purchase.
Attestation of Compliance (AOC)	Documented evidence that a supplier has upheld security best practices to protect cardholder data. It is testimony that a supplier successfully demonstrated exceptional security best practices to secure cardholder data.
Auxiliary Approver	A person authorized by a campus delegation of authority (DOA) to review a transaction (contracts, etc.) before the DOA can approve.
Campus Information Security (InfoSec)	The information security team secures data, systems, and devices at each campus. This includes developing policies, tools, and programs to prepare systems and services for potential emergencies.
Contract Party	The participants of a contract, designated as the first party (UMass) and a second party (the Supplier) for the contract on UMass CFS.
Contract for Service (CFS)	An agreement between UMass and an individual or entity wherein UMass agrees to pay the individual or entity for services to be provided.
Delegation of Authority (DOA)	The University's Delegation of Authority details University personnel authorized to bind the University to contracted terms and conditions with external parties.
Group Purchasing Organization (GPO)	An entity that negotiates favorable contracts on behalf of its members. i.e., MHEC (Massachusetts Higher Education Consortium).
HECVAT	The HECVAT, or Higher Education Community Vendor Assessment Tool, is a questionnaire framework designed to help institutions of higher education measure their vendor risk. HECVAT was developed by EDUCAUSE's Higher Education Information Security Council (HEISC), a team devoted to security, data governance, and compliance in higher education.

HITRUST	HITRUST, or Health Information Trust Alliance, was created and maintains the Common Security Framework (CSF), a certifiable framework that UMass references to help organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner.
Internet Protocol address (IP address)	A numerical label such as 192.0.2.1 is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: network interface identification and location addressing.
ISO2701 Report	The report, provided by an external auditor, provides insight into whether a supplier has an Information Security Management System (ISMS) - which is a program for establishing, implementing, maintaining and working to continually improve their InfoSec practices.
KPMG	KPMG is the official external auditor of the UMass system. Each Campus Controller's office needs to be aware if we are engaging with them for any other work.
Master Service Agreement (MSA)	A set of standard Terms and Conditions that can be used for multiple campuses or Systemwide – in this instance, a unique Statement of Work (SOW) or Scope of Services is drafted and linked to the MSA so that the terms apply, but the PO is unique to the Stakeholder who wrote the SOW.
No-Bid Justification (NBJ)	An exception to competitive procurement that justifies why you need to purchase from a specific supplier without going through a formal competitive bid process as required in the UMass Procurement Policy. Formerly known as the Sole Source process.
Office of General Counsel (OGC)	UMass group that advises and provides guidance on numerous issues to ensure that the University acts in accord with state and federal law and regulations, applicable University procedures, and best practices.
Office of Management (OOM)	Specific to UMass Chan Medical School, OOM works collaboratively with the campus to help address and resolve on-campus risk management and legal issues.
Payment Card Industry (PCI)	Half of the compliance standard PCI-DSS or Payment Card Industry Data Security Standard. The standard is a framework that defines the types of security required to ensure that payments, when accepted, transferred, stored, and processed, are secured responsibly.
PCI QSA Attestation	A PCI Attestation of Compliance (AoC) is a declaration of an organization's compliance with PCI DSS. It serves as documented evidence that the organization's security practices effectively protect against threats to cardholder data. This document must be completed by a Qualified Security Assessor (QSA) or the business's merchant.

Personally Identifiable Information (PII)	Any data that can be used to identify, contact, or locate a single person such as names, birth dates, social security numbers, etc.
Protected Health Information (PHI)	Any data that can be used to associate a person's identity with their health care such as health plan, beneficiary numbers, device identifiers, serial numbers, biometric identifiers, etc. Learn more about PCI, PII, and PHI
Real Property (Real Estate)	Includes (but is not limited to) land, buildings, air rights, water rights, and mineral rights owned by the University and is property of the Commonwealth of Massachusetts, which has been entrusted to the University for stewardship. All procurement transactions related to Real Property must comply with the Capital Planning, Land and Facilities Use Policy (T93-122, as amended).
Renewal	Renewals should be triggered by the original contract renewal terms. For example, a contract may be extended for 2 one-year periods at the end of the original term as indicated in the original terms.
Second Party	The individual or entity/organization that the University is entering into the contract with.
Statement of Work (SOW)	A contract type used for a specific service/project when an MSA already exists with the supplier/vendor. It is a comprehensive legal document that details the specifics of the project/service including scope, deliverables, timeline and should always be linked to an MSA.
Scope of Service (SOS)	Used to gather and agree on scope details to be included in any purchase agreement i.e., Purchase Order (PO), Contracts for Services (CFS), SOW, or MSA. It details the overall objective and description of the work a supplier/contractor will provide.
SOC2 Report	SOC reports are the output provided by an external auditor documenting internal financial controls around information that impacts financial statements. SOC2 reports put a higher focus on the cybersecurity aspect of an organization. This includes information security, availability, process integrity, confidentiality, and privacy controls.
Sub-Award/Sub-Contract	When a portion of UMass' sponsored project is passed through to another entity in order to complete a portion of the sponsored project's scope of work. Please reach out to your campus grant accountant in the Controller's Office for additional questions.
University Official	The University Official exercising managerial and budgetary control for the Contract. The individual named in the contract has responsibility for the performance of this contract. This individual is also the primary contact for the supplier as it relates to this contract.
Vendor Breach Notification Policy	A set of guidelines that dictate how a company will handle and report data breaches. This provides insight into how/when the vendor in question has committed to informing their clients should a breach occur.

Vendor Cloud/Hosting Provider Security Attestation	Host Attestation Service checks by validating a compliance statement (verifiable proof of the host's compliance) sent by each host against an attestation policy (definition of the secure state). This ensures the cloud/host environment the vendor is utilizing has been verified as secure.
Vendor Privacy Policy	A privacy policy document states whether and in what manner a site gathers, utilizes, disseminates, or monetizes the personal data of its visitors. These documents are required under most global laws, such as the GDPR, CPRA, and LGPD.