UNIVERSITY OF OKLAHOMA
University Payment Card Security Policy

Subject:	University Payment Card Security Policy	**Coverage:**	The University of Oklahoma—All Campuses
Regulation:	PCI DSS, FACTA, GLBA, State of Oklahoma Information Security Policy, Procedures, Guidelines	**Version:**	1.0.0
		Approved:	07/25/2012
Effective:	07/25/2012	**Revised:**	Initial Document

Policy Summary:	The University has established security standards and processes for the protection of Cardholder Data in compliance with the Payment Card Industry Data Security Standard (PCI DSS). PCI requirements apply to all OU entities that collect, store, process, or transmit Cardholder Data, provide for its oversight, or support an entity that does. Each such entity will be required to comply with the established processes and standards.
Purpose:	To establish organizational level security standards for the protection of Cardholder Data and compliance with Payment Card Industry Data Security Standards.
Policy:	University entities that collect, store, process, or transmit Cardholder Data must be approved and authorized by the Office of the Bursar for processing payment card transactions. All OU entities that collect, store, process or transmit Cardholder Data, provide for its oversight, or support an entity that does will comply with all requirements of the PCI DSS and the respective Campus Payment Card Security Standard.
Documentation:	All material supporting information and evidence collected and/or used as part of the compliance process will be formally documented and securely maintained.
Scope/Applicability:	This policy covers all University campuses and applies to all OU entities that collect, store, process, or transmit Cardholder Data, provide for its oversight, or support an entity that does.
Regulatory Reference:	Payment Card Industry (PCI) Data Security Standard, 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (‘‘GLB Act’’), Fair and Accurate Credit Transactions Act of 2003; State of Oklahoma Information Security Policy, Procedures, Guidelines
Consequences of Non-compliance:	Failure to comply may result in the termination of a merchant’s ability to accept payment cards and/or fines assessed by the Offices of the Bursar.
Policy Authority:	This policy is authorized and approved by the Office of the President.
Policy Compliance Audit:	The University’s Internal Auditing department is responsible for the auditing of compliance with this policy.
Policy Enforcement:	The Offices of the Bursar are responsible for enforcement of this policy.
Related Standards:	OUHSC Payment Card Security Standard; OU-Norman Payment Card Security Standard; OU-Tulsa Payment Card Security Standard
Renewal/Review:	This policy is to be reviewed and updated as needed.