3.7 All confidential and sensitive data will be retained only as long as required for legal, regulatory and business requirements and in a secured location (e.g. locked cabinet/safe). Cardholder “authorization data”, including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction. After authorization, the data must be destroyed via cross shredding or pulping by using the University approved confidential waste service. Storage of cardholder authentication data post-authorization is prohibited..

Version	Revision Date	Summary of Changes	Approvals
1.0	June 2016	Initial draft	