MDRP Responsibilities Checklist

Any department accepting payment cards on behalf of Middlebury for gifts, goods or services (“Merchant Department”) must designate an individual (staff or faculty member) within that department who will have primary authority and responsibility for eCommerce and payment card transaction processing within that department. This individual will be referred to in the remainder of this policy statement as the Merchant Department Responsible Person or “MDRP”.

All MDRPs must:

_____ Ensure that all staff, contractors, student workers, volunteers, hereinafter referred to as agents of the College, complete the PCI Security Awareness Training & Agreement, http://go.middlebury.edu/pcidss upon hire and annually. A current listing of completed trainings is available at http://go.middlebury.edu/pcitrainingspreadsheet.

_____ Verify and collect PCI DSS Compliance documentation, in accordance with the Service Provider Management tab, for Service Providers on an annual basis or upon major changes. The MDRP should retain a copy of the Attestation of Compliance (AOC) and submit a copy to the PCI DSS Compliance Team upon receipt.

_____ Validate compliance for the merchant department on an annual basis, by completing the Self-Assessment Questionnaire in collaboration with the PCI Compliance Team.

_____ Ensure user access to cardholder data environment is revoked (notify the pcicomplianceteam@middlebury.edu) when the individual’s job no longer requires access to the cardholder data environment. Maintain an audit log of user access to cardholder data environment for a minimum of one year.

_____ Be aware of all payment processes and practices within your merchant department. It is the responsibility of the MDRP to ensure Standard Operating Practices are known by all in your department, are adhered to, are in accordance with the PCI DSS and are approved by the PCI Compliance Team.

_____ Initiate the process in the event of a security incident or breach, see Security Breach Response

Payment Card Terminals and Point of Sale (PoS) Devices:

_____ Ensure all devices accepting payment card data are maintained under a state of consistent control and supervision.

_____ Ensure Point of Sale devices/terminals (cash registers, stand-alone swipe terminals etc.) are physically secured.

_____ Complete a Terminal Characteristics form and Monthly Physical Inspections for tampering or substitution. Systems not in use must be secured in a locked facility and regularly inventoried. Monthly Physical Inspection forms must be forwarded to the PCI Compliance Team upon completion of monthly inspections.

_____ Ensure that all agents of the College are trained on tampering and skimming prevention upon hire and at least annually. Please see Physical Security and Skimming Prevention.

_____ Please read the Middlebury PCI Policy for Credit Card and eCommerce Payments for additional responsibilities.

Individuals found to have violated the Middlebury PCI Policy for Accepting Credit Card and eCommerce Payments and the PCI WISP, whether intentionally or unintentionally, may be subject to disciplinary action including termination and could limit a department’s payment card acceptance privileges.