UNIVERSITY OF CENTRAL FLORIDA

Office of Research and Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246

Annual Security Training Briefing 2017

Acknowledgment Receipt

I acknowledge receiving "UCF's Annual Security Briefing" by the Office of Research and Commercialization which described my continuing responsibility to safeguard classified information. I understand that my signature below affirms I understand the contents of the Annual Security Briefing and Insider Threat Training.

Employee Signature: _____

Employee Printed Name: _____

Date: _____

The National Industrial Security Program Operating Manual (NISPOM) **3-108. Refresher Training.** The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. See paragraph **8-103c** of chapter 8 of this Manual for the requirement for IS security refresher training. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors shall maintain records about the programs offered and employee participation in them. This requirement may be satisfied by use of distribution lists, facility/department-wide newsletters, or other means acceptable to the FSO.

NISPOM Reference:
8-103c. All IS users will:
(1) Comply with the ISs security program requirements as part of their responsibilities for the protection of ISs and classified information.
(2) Be accountable for their actions on an IS.
(3) Not share any authentication mechanisms (including passwords) issued for the control of their access to an IS.
(4) Protect authentication mechanisms at the highest classification level and most restrictive classification category of information to which the mechanisms permit access.
(5) Be subject to monitoring of their activity on any classified network and the results of such monitoring could be used against them in a criminal, security, or administrative proceeding.

3-103b. Insider Threat Training. All cleared employees must be provided insider threat awareness training before being granted access to classified information, and annually thereafter. Training will address current and potential threats in the work and personal environment and will include at a minimum:
(1) The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee.
(2) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within ISs.
(3) Indicators of insider threat behavior, and procedures to report such behavior.
(4) Counterintelligence and security reporting requirements, as applicable.