VERTEX AEROSPACE CORPORATE 2020 ANNUAL SECURITY REVIEW

FOREWARD

The purpose of this training is to provide Vertex employees a sound basis for security measures for the protection of government customer information, the protection of company and personally owned things, but most importantly, the protection of our employees; our most valuable asset. This training specifically covers:

- Initial and annual cleared employee security briefing
- The Standard Form (SF) 312
- Reporting of Adverse Information to Security
- The protection of classified information
- Operational security and secure communications
- Counterintelligence and defensive security
- International Travel
- the company's Insider Threat program
- a review of the Workplace Violence Plan
- the protection of CUI/FOUO information, as well as the
- protection of Company Proprietary Information

For all Vertex employees that will handle PII, PHI, and log into a US Government Automated Information System (a dot mil computer system), please complete the following training.
https://securityawareness.usalearning.gov/cybersecurity/index.htm

You will need to save as a PDF to print your certificate
https://securityawareness.usalearning.gov/piiv2/index.htm

The training certifications are auditable and must be maintained by the employee using that system.

This briefing meets your requirement for ANNUAL refresher training and serves as the initial for new employees.

Waiver Criteria: None. This annual training is mandatory for all interim or final cleared employees at the CONFIDENTIAL, SECRET, or TOP SECRET level, as well as cleared consultants that possess DoD issued Security Clearances.

***Failure to complete this training can result in the removal of your clearance/access through the Security Office.**

For questions concerning this training, please contact Robert Hayes at 601-607-6342 or by email, Robert.Hayes@vtxaero.com

Contents

Security Poster Requirements

The Ethics and Security poster is required to be displayed as a reminder to our employees of Vertex Aerospace's commitment to maintain the highest level of ethical conduct in all aspects of our business.

The poster is a reminder to report violations or concerns to Vertex Security Officers.

SF312-Nondisclosure Agreement (for all cleared employees)

What did you sign? A contractual, LIFETIME agreement between the U.S. and employee or contractor that informs the subject of (a) the trust that is placed in them by granting them access to classified information; (b) their responsibilities to protect that information from unauthorized disclosure; and (c) the consequences that may result from failure to meet those responsibilities.

Proprietary Information Protection

What do we want to protect?

- Technical Data
  - Parts Lists
  - Drawings
  - Bills of Material
  - Process Documents
  - Analyses
  - Specifications
- Government-Regulated information (ITAR or EAR)
- Purchase Orders/Supply Chain
- ANY customer documentation
- ANY item with a Vertex Proprietary, or ITAR/Export-Controlled material statement on it
- Personal Identifying Information (PII)
- Don't make it easy for an outsider to build up a picture of our organization and use it against us

Personally Identifiable Information (PII):

"Information which can be used to distinguish or trace an individual's identity; such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, race, religion, mother's maiden name, etc." Other examples of information that could distinguish an individual include, but are not limited to, passport number, driver's license number, taxpayer identification number, patient identification number, financial account or credit card numbers, and address information.

Protected Health Information (PHI):

Individually identifiable health information that is a subset of health information, whether oral or recorded in any form or medium, including demographic information collected from an individual. Additionally, PHI is the individually identifiable health information that: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

***PII information should only be transmitted outside the company network when it is encrypted to 256 bit AES encryption with a strong password. Passwords shall never be included in the body of a transmission along with the encrypted information.**

Classified Information

Classified information is official information that has been determined, pursuant to E.O. 12958 or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. Classified information is US GOVERNMENT PROPERTY.

Safeguarding Classified Information

Approved Computer Systems:

Processing of classified information must be performed only on computer workstations and systems formerly approved by the government.

Proper Storage and Protection:

Classified material, when not in use, must be stored in approved containers: such as safes, vaults, or closed areas that are frequently patrolled or are equipped with alarm systems.

- Always report evidence of tampering and attempted illegal entry into a secure container
- Perform area checks to ensure classified material has not been left unattended

Classified material must be kept under constant surveillance. Work in a secure area, with doors closed, blinds drawn, and signs posted. Cover all classified material when in the presence of unauthorized personnel. Return classified documents to storage containers when no longer needed or by the end of each day, at the latest. Classified information may not be removed from official premises without proper authorization.

Access to Classified Information:

May be granted only if you need to know to perform his or hers job and if the recipient has a valid security clearance.

Secure Communications:

Correct use of secure communication devices can reduce the vulnerability of leaking sensitive and classified information.

Did you know?

You are personally liable for unauthorized release of classified information.
Penalties could be, but are not limited to:

- **Loss of monetary gains made from improper disclosure**
- **Loss of security clearance**
- **Termination of employment**
- **Criminal prosecution (prison/fines)**

General Guidelines for Secure Communication

- The secure communications device is an unclassified cryptographic item
- The device remains in an unclassified state until a user inputs his/her authorized PIN
- After a PIN has been input, the device is classified and should be protected as such
- Carefully follow all instructions to place a secure call. Do not discuss any classified information if there is any questions of validity
- All mobile phones, two-way pagers, two-way radios, personal digital assistants (PDAs), or any other recording devices should be turned off and removed from the area before any call is made. If a conference phone is in the area please ensure it is properly unplugged before any calls are made
- The device is not to be taken from the approved facility for use at a residence or unauthorized business environment

Protection & Marking

All Classified documents must be clearly marked to indicate the degree of Protection. Classified information requires protection in the interest of National Security.

Markings:
Must be placed on the front of each document and/or disks.

Identification Markings:
All material from the Madison facility must show the name and address of the facility responsible for its preparation and the date of preparation.

Overall Markings:
The highest degree of classification must be marked or stamped at the top and bottom of the outside front and back cover.

Page Markings:
Interior pages of classified documents must be marked at the top and bottom of that page

Marking and Destruction

Portion Markings: classified document must be marked to indicate the level of classification of that portion.

(TS) Top Secret **(C) Confidential**
(S) Secret **(U) Unclassified**

Illustrations:
All images will be appropriately marked and will not be abbreviated and will be prominently placed on or near the illustration.

Table of Contents and List of Illustrations/Tables:
The classification symbol must be placed immediately before and to the left of the heading or title.

Destruction:
Classified material must be destroyed using approved classified destruction methods.
Controlled documents must be turned in to Security for destruction.

Security, Training, Education and Professionalization (STEPP) Portal Page:
https://cdse.usalearning.gov/login/index.php

Controlled Unclassified Information (CUI)

CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Two types of CUI

- CUI Basic
  - •Laws, Regulations, or Government-wide policies which DO NOT require specific protections
- CUI Specified
  - •Laws, Regulations, or Government-wide policies which REQUIRE specific protections
    - Unique Markings
    - Enhanced Physical Safeguards
    - Limits on who can access the information

Safeguarding

- CUI must be stored or handled in controlled environments that prevent or detect unauthorized access
- Sealed envelopes
- Areas equipped with electronic locks
- Locked doors, overhead bins, drawers, file cabinets
- Existing Best Practices
  - Policy and Procedures
  - Training and awareness
  - Physical and Electronic protections
  - Oversight Measures
  - Reporting

Adverse Information

As a general rule, this is information which reflects adversely upon the integrity or character of the employee and suggests his or her ability to safeguard classified information could be impaired.

Reporting Requirements:

As a cleared employee, you have a mandatory obligation

- Report security violations or infractions
- Report suspicious contacts, whether it is an inquisitive co-worker, friend, family member or strangers
- An arrest for any offense
- Filed for Bankruptcy or Chapter 13
- Report changes in employee status such as a name change, change in employment status, or other personnel action affecting your security record
- Report any involvement with another person or firm where you would be considered a Representative of a Foreign Interested
- Report adverse information, whether on yourself or another cleared employee
- Report foreign travel using the Vertex Travel Portal

Company Computer Security

- **Vertex reserves the right to exclude Internet access to irrelevant sites**
- **Use computers for authorized business purposes only**
- **Do not open e-mail attachments from unknown sources**
- **Do not use a personal email to communicate business**
- **Never share passwords with anyone**
- **Avoid copyright infringement**
- **Secure hardware**
- **Preserve your work**
- **Use discretion when accessing company and/or customer provided internet and email**
- **Do NOT process classified information on unapproved systems**
- **Computer assets not controlled or managed by Vertex entities cannot be connected to the Vertex network**

Insider Threats

Acts of commission or omission by an insider who intentionally or unintentionally compromises or potentially compromises DOD's ability to accomplish its mission. These acts include, but are not limited to, espionage, unauthorized disclosure of information, and any other activity result in the loss or degradation of departmental resources or capabilities.

What is a threat?

America's role as the dominant political, economic, and military force in the world makes it the number one target for espionage. In addition to the intelligence services of both friendly and unfriendly countries, sources of the threat to classified and other protected information include:

- Foreign or multinational corporations
- Foreign government sponsored educational and scientific institutions
- Insiders
- Extremist ethnic or religious organizations
- Freelance agents
- Computer hackers
- Terrorist organizations
- Revolutionary groups
- Organized crime
- Terrorism
- Foreign Intelligence Espionage
- Targeting the U.S. Government and U.S. Corporations (both Classified and FOUO/Proprietary)
- Proliferation of advanced conventional weapons or weapons of mass destruction
- Targeting of National Information Infrastructures
- Drug syndicates

What is an "Insider Threat?"

- Defined as one or more individuals with the access and/or inside knowledge of a Company, Organization, or U.S. Government that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm
- Companies victimized by current or former employees can incur costs from $5,000 to $3M
- The FBI works closely and partners with businesses (including Vertex) to investigate and determine if suspected insiders are guilty of violating Economic Espionage laws to include Theft of Proprietary/Intellectual Property
- Vertex has established a formal Insider Threat Program, which is led by Robert Hayes, the Insider Threat Program Manager

Behavioral Indicators:

- Disregards company policies/procedures
- Engages in suspicious personal contacts: such as with competitors, business partners, or other unauthorized individuals.
- Depression
- Stress in personal life
- Exploitable behavior traits:
- Use of Alcohol or Drugs
- Gambling
- Infidelity in Marriage
- Financial troubles
- Disciplinary issues

Potential Espionage Indicators:

- Failure to report overseas travel or contact with foreign nationals
- Seeking to gain higher clearance or expand access outside the job scope
- Violating the "need-to-know" principle
- Working hours inconsistent with job assignment or insistence on working in private
- Exploitable behavior traits (blackmail)
- Repeated security violations
  - Attempting to enter areas not granted

The threat an insider will use is his or her access, wittingly or unwittingly, to do harm to the security of the Company or to the United States. This threat includes damage through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of government, company, contract or program information, resources, or capabilities.

Insider Threats

Motivating Factors

- Greed or Financial Need
- Anger/Revenge
- Problem at Work
- Ideology/Identification
- Divided Loyalty
- Family Problems
- Adventure/Thrill
- Vulnerability to blackmail
- Ego/Self-image
- Ingratiation
- Compulsive and Destructive Behavior

Collection Methodologies

- Requests for Information
- Solicitation or Marketing of Services
- Physical Acquisition of the Technology
- Public Venues such as a conference or tradeshow
- Foreign Visitors
- Cyber Attack / Hacking of Mobile Phones
- Foreign Targeting of U.S. Travelers Overseas

Deflecting Elicitation Attempts

Any suspicious situation should be reported to security immediately.
Allow Security the opportunity to investigate the situation, as it is our expertise!

What should you do when someone is asking you about your job, the facility, the company, or a program?

- Refer them to public sources (websites, press releases)
- State that you would have to obtain approval from Security to have such discussions or give them the Security Office phone number.
- Change the topic and/or deflect their question with one of your own.
- State that you are unsure of what they are talking about or tell them you don't know the answer.
- Respond with "Why do you ask?"
- Give a nondescript answer.
- State that you cannot discuss the matter.
- Ignore any question or statement you think is improper.
- Never confirm nor deny!

"See Something…Say Something!"

Reporting Requirements

- Be cognizant of suspicious behaviors of other employees and report them as soon as possible to the FSO and/or the appropriate USG law enforcement official
- Employees should be aware of the Counter Intelligence connections and risks that are connected to the insider employee that already has program access
- Per DoD Directive 5240.06, personnel who fail to report foreign intelligence contacts and reportable activities, indicators, and behaviors are subject to punitive action

For Additional Insider Threat Training Please Visit:
http://cdsetrain.dtic.mil/itawareness/index.htm

Foreign Intelligence/Threat Awareness

The defense industry reporting continues to reflect increasing trends of foreign collection activity involving proprietary strategic management information, to include bid proposals, price structuring, business processes, and marketing plans. With the reputation as one of the United States' top DoD contractors, the profile of Vertex Aerospace is heightened and well known.

Employees should report the following to their FSO immediately:

- Any foreign requests for U.S. Defense/Technical documents, papers, manuals, or related information, whether or not these items are classified or sensitive
- Any proposals for joint ventures
- Requests by any individual (regardless of nationality) for illegal or unauthorized access to U.S. Government classified, proprietary or otherwise sensitive information

The Ongoing Threat

Methods include assessment, elicitation, eavesdropping, technical eavesdropping, bag operations, surveillance, theft of info, intercepting electronic communications, and phishing via e-mail and telephone.

5 General Categories of Information Collection Methodologies:

1. Human Intelligence uses people to gather information. Including: visits to facilities, unsolicited requests for information, seeking employment, and targeting at seminars, conventions and exhibits
2. Signals Intelligence involves the collection of electronic signals (phone calls and e-mails).
3. Imagery Intelligence uses all variants of images to collect information
4. Open Source Intelligence gathers information that is legally and publically available, including information from the news media and Internet
5. Measures and Signatures Intelligence is technically derived intelligence that uses the unique characteristics of fixed and dynamic target sources

Counter Intelligence (CI)/Defensive Security

A proactive discipline that deters and detects attempts by a foreign government, agent or competitor from illicitly acquiring national security-related information or technology. Its mission is to protect classified or proprietary technology from compromise.

Know what you are protecting: The ASSET

- An asset to the U.S. Government is any person, facility, material, information, or activity, which has a positive value to the U.S. Government or a company. The asset may have value to an adversary as well
- You represent the first line of CI defense against those who seek to deny the U.S. of our competitive advantage
- Suspicious contacts include, but not limited to, any efforts to gain illegal or unauthorized access to classified information or to compromise a cleared employee
- Cleared defense contractors must submit suspicious contact reports (SCRs) to their Industrial Security Representatives (ISRs). ISRs, after initial review, provide those SCRs to the DSS CI Office

Indicators and Countermeasures

Request for Information

Indicators:

- Sends request using foreign address
- Assures that export license are not required
- Fails to identify end user
- Identifies employer as foreign government

Countermeasures:

- View unsolicited requests with suspicion
- Respond only to people who are known
- Do not respond if requestor cannot be verified.

Targeting

Indicators:

- Personnel receive an all-expenses paid invitation to lecture in a foreign nation
- Telephone monitoring and hotel room intrusions
- Attendees wear false name tags
- Individual returns to same booth multiple times

Countermeasures:

- Consider what information is being exposed
- Provide detailed travel briefing
- Request threat assessment from program office

International Travel Process:

1. Submit travel approval form through the automated process located on the VTX LAN under the Security Tab.

2. Travel approval form is signed by a Security Representative and the travel briefing for specified country is sent to the employee.

3. All International travel has to be pre-approved by Security before departure date.

4. All travel to Extreme Risk Locations will also have to be submitted to and pre-approved by the Vertex Aerospace Security Director and requires a Personal Protection Plan.

Why We Track It:

- To protect Vertex employees traveling outside of the continental United States

- To locate employees and the dependents in the event of an emergency

International Travel

As soon as an employee receives their travel itinerary, they have to complete the online International Travel Program Approval Form. After acquiring the appropriate signatures, the form is submitted to the Security Departments

Once the form is received, the employee will receive an International Travel briefing for the country he/she will be traveling to.

- Information about the country you are traveling to
- travel policies & procedures
- All employees travelling Internationally are required to notify Vertex Corporate Travel within 8 hours of landing at their final destination. Traveling employees should immediately check in if there is an attack, earthquake, tsunami, or pandemic.
- For cleared employees. the "Counter Intel Debriefing" must be completed and submitted to the Security Department upon return from travel
- Vertex has a corporate web page with travel related resources (i.e. contacts, booking profiles, lodging, transportation, policies, forms, alerts, etc.)
- Security also has an internal web page for security travel training videos
- United States Department of State's web page of current travel alerts: http://travel.state.gov/travel/cis_pa_tw/pa/pa_1766.html
- United States Department of State's web pages for country-specific information: http://travel.state.gov/travel/cis_pa_tw/cis/cis_4965.html

Foreign Visits

Suspicious contact during a foreign visit can occur at any time.

Indicators:

- Request for information outside the scope of what was approved for discussion
- Hidden agendas associated with purpose of visit
- Visitors requesting information
- Wandering visitors
- New visitors added to group at last minute

Countermeasures:

- Contractors coordinate with DSS prior to visit
- Prior to visit, brief hosts and escorts on approved procedures
- Escort visitors at all times
- No recording devices allowed, to include cell phones

Elicitation and Recruitment

Intelligence officers spot and assess individuals for potential recruitment.

Indicators:

- Strategic use of conversation to subtly extract information about you, your work, and your colleagues
- Explore potential weaknesses which may be used against you, to include:
  - Drugs/Alcohol
  - Gambling
  - Adultery
  - Financial Problems

Countermeasures:

- Do not share anything the elicitor or recruits is not authorized to know; change topic, deflect question, provide vague answers
- Report incident to your FSO

Facility Visitors

All cleared Vertex Corporate locations have stringent rules for persons visiting the facilities (Madison, Warner Robins, Crestview, and Newport News). The security team uses an electronic visitor management process for the vetting of all persons into these facilities including new employees, short- and long-term visitors, as well as foreign national persons. Failing to adhere to the visitor control processes can put the company at risk with US Government regulations. Contact your local FSO if you need to bring a visitor into a facility.

Badge Recognition

Every person on the facility is required to wear a CA issued badge waist high and visible at all times.

- Purpose

  Identify
  - The person as a visitor or employee
  - If the person is a US Citizen or Foreign visitor
  - Whether or not they have escorted or unescorted access
  - Security
  - Minimize unauthorized access
  - Accountability
  - Of all personnel on-site

Remember: All Temp and Visitor badges must be turned in everyday prior to departure. Report all lost, stolen or misplaced badges immediately.

Prohibited and Controlled Items for Physical Security

Prohibited

- Alcohol/drugs
- Explosives
- Guns
- Ammunition
- Bio or Chem Warfare Agents
- Stun Guns
- Grenades
- Knife (>2.5")
- Fireworks
- Bow/Arrows
- Swords

Controlled

- Personal Cell phones with cameras
- Laptops
- Two-way Radios
- Tape/voice Recorders
- Thumb drives
- RF Transmitting Equipment
- Recording Equipment
- Controlled Substances

Technology Control Plan (TCP)

- Established in accordance with Corporate Policy
- Define the requirements to control access to technical information by Foreign Nationals

Exports

- Are defined under the Code of Federal Regulations (CFR) and the International Traffic and Arms Regulations (ITAR)
- Disclosure to a Foreign National in the course of employment or temporary assignment at a US company may result in an export violation

Disciplinary Actions for Security Violations

- The company has instigated a graduated disciplinary process in accordance with Section 1-304 of the NISPOM and ISL 2016-02.
- This guideline applies to all security violations and infractions.
- Please refer to the HR disciplinary guidelines for greater detail and further information.

Social Media

Social media provides a false sense of security and has more risks than perceived. Protect yourself from disclosing too much or trying to impress potential friends or associates.

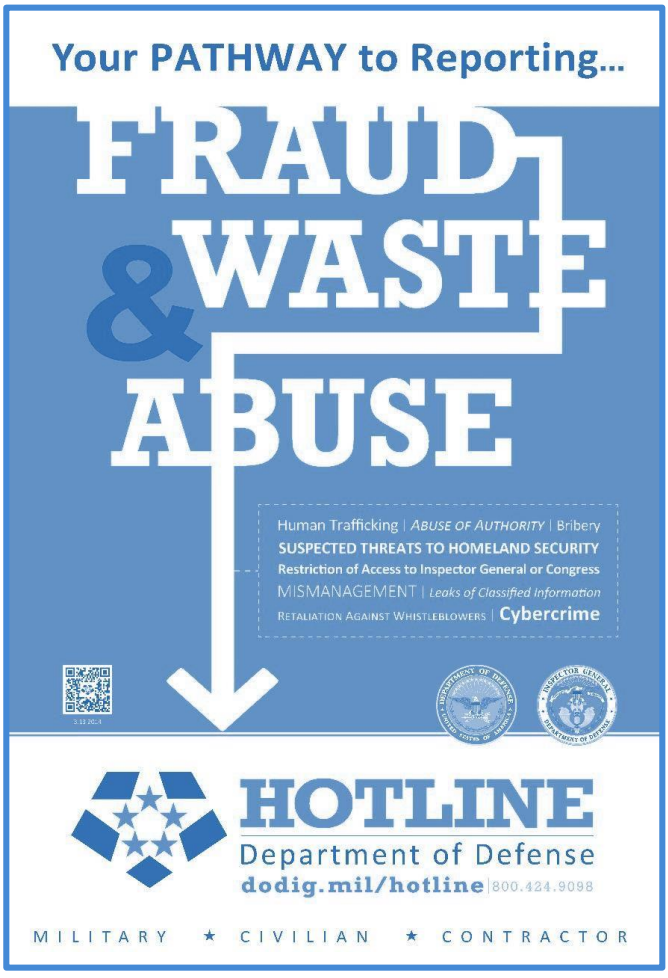
Common Social Media Risks

- Personal information used for social engineering attacks
- Predators forming online relationships
- Harvesting your personal information to impersonate trusted friends/institutions
- Attackers use social media sites to distribute malicious code
- Attackers can create custom apps that appear innocent
- *Geo-tagging*

Protect Yourself from Social Media Risks

- Limit the personal information you post
- Remember it's a public resource
- Be wary of strangers & skeptical
- Evaluate your app privacy settings
- Check privacy policies
- Be wary of third-party apps
- Use strong passwords
- Keep software/browsers up to date
- Use and maintain anti-virus software

DoD Guidelines: Staying Safe on Social Media
https://www.us-cert.gov/ncas/tips/ST06-003



DoD Hotline Phone:
800-424-9098
703-604-8799
664-8799 (DSN)
Hotline Fax:
703-604-8567

DOJ Hotline Phone:
800-869-4499
Hotline Fax:
202-616-9881

Southwest Asia Hotline:
877-363-3348
664-1151 (DSN)
www.dodig.mil/hotline

Workplace Violence Awareness

Warning Signs

- Visible Stress
- Excessive Anger
- Low Morale
- Physically violent
- Abusive or Intimidating
- Unusual or bizarre behavior
- Major changes in habits
- Extreme mood swings

Prevention

- Foster communication
- Make eye contact
- Give the individual your full attention
- Speak in a calm voice
- Let the person vent and listen attentively
- Inform your supervisor of on-going problems which you believe have a potential for violence
- Contact HR or Security

VERTEX WORKPLACE VIOLENCE RESPONSE PLAN

In accordance with Vertex Policy and Procedure SI 1.003 Workplace Violence, the following plan shall be allowed in the event of workplace violence at all Vertex Aerospace locations.

Reporting Workplace Violence: Workplace violence is defined as violent acts occurring at the workplace or originating with employees/employers that threaten employees or other attendant persons. Any threatening act, whether written, spoken, or perceived must be immediately reported to the local security manager. If imminent danger exists, local law enforcement must be informed as soon as possible.

All-Call Message: Once a critical workplace violence incident is identified, it is the responsibility of the senior site security manager and/or leadership team member to initiate an 'all-call' message detailing what is known about a potential or in-process workplace violence incident. All-call messages include email, intercom, telephone, and text notifications to all site employees. The message should include information on the specific incident, location, and involved persons (with descriptions if possible) so that employees can decide how to best avoid the threat area.

RUN, HIDE, FIGHT: All workplace violence incidents are different and can change dramatically in the scope and nature during the event. **Run, Hide, Fight** is the standard responses to workplace violence. It is a range of decisions for the intended victim that must be continually reevaluated as a situation develops.

1) **RUN**. Employees should always try to get away or escape from the perpetrator as the first and most effective way of achieving safety. Running is your first decision.

2) If running will not work, then **HIDE**. Hiding can mean being out of sight under your desk or moving to an office and locking (and barricading) doors.

3) If running and hiding does not work, then **FIGHT**. As a last resort, if your life is in danger, fight back.

4) After hostilities or imminent threat cease, employees may not re-enter any part of the facility without the expressed approval of the senior Human Resources manager on-site and then, only after Law Enforcement investigators have released control of the facility back to the company.

All employees shall familiarize themselves with the local Vertex Headquarter facilities including public access locations and secondary exits/entryways so they may exit the facility in an emergency situation if they believe the situation dictates.

Training: All Vertex employees are required to review this plan annually. Take one half-hour of workplace violence prevention and identification training at least annually. This training shall be facilitated by the local facility security personnel and may consist of lectures, videos, trend data, local policy requirements, and specific threat identification. Program managers are required to ensure compliance with this training requirement for their employees.

REMEMBER RUN, HIDE, FIGHT

All-Call Message: Once a critical workplace violence incident is identified, it is the responsibility of the senior site security manager and/or leadership team member to initiate an 'all-call' message detailing what is known about a potential or in-process workplace violence incident. All-call messages include email, intercom, telephone, and text notifications to all site employees. The message should include information on the specific incident, location, and involved persons (with descriptions if possible) so that employees can decide how to best avoid the threat area.

RUN, HIDE, FIGHT: All workplace violence incidents are different and can change dramatically in the scope and nature during the event. **Run, Hide, Fight** is the standard responses to workplace violence. It is a range of decisions for the intended victim that must be continually reevaluated as a situation develops.

1) **RUN**. Employees should always try to get away or escape from the perpetrator as the first and most effective way of achieving safety. Running is your first decision
2) If running will not work, then **HIDE**. Hiding can mean being out of sight under your desk or moving to an office and locking (and barricading) doors
3) If running and hiding does not work, then **FIGHT**. As a last resort, if your life is in danger, fight back
4) After hostilities or imminent threat cease, employees may not re-enter any part of the facility without the expressed approval of the senior Human Resources manager on-site and then, only after Law Enforcement investigators have released control of the facility back to the company

Contact Your Local Security Officers

NAME	TITLE	LOCATION	PHONE #
Robert Hayes	FSO	Vertex Madison/Crestview	601-607-6342
Wilson Justin	FSO	Flight Int.	757-503-2720
Lawrence Davis	FSO	TCS	478-449-8032

Thank you for your participation in the 2020 Annual Security Refresher Training!