

# Personnel Security

Dr. Shahzada Khurram

# Personnel Security

Humans are the weakest link in the security chain

- **Job Descriptions**
  - First step in defining security needs related to personnel
  - Defines the roles to which an employee needs to be assigned
  - Defines the type and extent of access the position requires
- **Separation of Duties**
  - Critical, significant, and sensitive work tasks are divided among several individual people
  - Helps protect against collusion
- **Job Rotation**
  - Rotating employees among multiple job functions
  - Provides knowledge redundancy
  - Reduces risk of fraud, data modification, theft, misuse
- **Cross-training**
  - Employees are just prepared for multiple job positions
  - Just helps on knowledge redundancy

# Employment Agreement

- Employment agreement must be signed before job responsibilities are provided
- **NDA:** Non-disclosure agreement – used to protect confidential agreement within an organization
- **NCA:** Non-compete agreement – used to prevent former employees to work for competitors
- **Mandatory Vacations:** places a different employee, helps detect fraud, abuse, negligence

# Employee Termination Process

- ✓ Should take place with at least one eye witness
- ✓ Once informed of termination, all access (logical/physical) should be disabled and the employee should be escorted out of office
- ✓ Best time to terminate is middle of the week at the end of the shift
- ✓ Before the employee is released, all organization-specific assets need to be collected
- ✓ Exit Interview should be conducted – primary purpose is to review the liabilities and restrictions placed on the former employee

# Employment Candidate Screening

- Should be based on criticality and sensitivity defined by the job description
- Should be completed before a candidate is onboarded into the organization
- Its an administrative control
- BG, drug test, credit score, criminal records, education, professional experience

- **Awareness** – Change user behavior - this is what we want, we want them to change their behavior.
- **Training** – Provides users with a skillset - this is nice, but if they ignore the knowledge, it does nothing.
- **Vendors, Consultants and Contractor Security.**
  - When we use outside people in our environments, we need to ensure they are trained on how to handle data. Their systems need to be secure enough for our policies and standards.
- **Outsourcing and Offshoring** - Having someone else do part of your (IT in our case) work.
  - This can lower cost, but a thorough and accurate Risk Analysis must be performed. Offshoring can also pose problems with them not having to comply with the same data protection standards.

Thank you