3.7.3 Employee Documents Facts

Employment agreements are the documents that explicitly identify the terms and conditions of employment. These agreements are included in the hiring policies established by an organization's Human Resources Department and increase the overall security of a computer network. The employee must agree to these terms and conditions and signify approval by signing the documents. All agreements must be signed before the employee begins work. Employee agreement documents are identified in the following table:

Agreement	Description
Non-Disclosure Agreement	The *non-disclosure agreement* (NDA) is a legal contract between the organization and the employee that specifies that the employee is not to disclose the organization's confidential or proprietary information to anyone outside the organization. This document is especially important as a deterrent to employee disclosure of sensitive information or secrets of the trade to competitors or even the general public.
Non-Compete Agreement	The non-compete agreement prohibits an employee from working for a competing organization for a specified time after the employee leaves the organization. Some non-compete agreements specify geographical locations in addition to or instead of time frames.
Ownership of Materials Agreement	The ownership of materials agreement specifies the organization's ownership of intellectual property created by the employee during the employment period.
Data Handling and Classification Policy	A data handling and classification policy documents the security classification levels of information and the guidelines for handling each level of classified materials. The policy should increase the awareness for data protection and provide rules for protecting the data.
Clean Desk Policy	A clean desk policy is designed to prevent confidential information being left where it is easily accessible. This requires employees to file all documents away and lock their filing cabinets. Nothing should be left out on desks any time an employee is not on their desk or when they are done using a document. This policy is in compliance with ISO regulations and the Data Protection Act. This regulation should be displayed around the organization with clear instructions of steps to be taken by employees. The regulation requires the employees to be responsible for all documents they handle and the organization to provide access to shredding and storage devices.
Acceptable Use Policy	The acceptable use policy (AUP) identifies the employee's rights to use company property, such as internet access and computer equipment, for personal use. The policy should define the activities that are acceptable and the activities that are not acceptable. This policy maximizes employee productivity and secures the organization's network from malicious and dubious websites and links. *Privacy* is individuals' rights to keep personal information from unauthorized exposure or disclosure. In a business environment, businesses might need to be able to monitor and record actions taken by employees. Such monitoring might be viewed as a violation of individual privacy. To protect against legal issues: ▪ Define the types of actions and communications that will be monitored. For instance, it is typical for a business to reserve the right to monitor all activities performed on company computers, even if those activities might be of a personal nature. ▪ Clearly communicate all monitoring activities. Users should know that monitoring is being performed. ▪ Apply monitoring to all employees. Targeting specific employees could be grounds for discrimination. ▪ Comply with all legal requirements for privacy. For example, personal medical information is protected and cannot be shared without prior authorization.
Password Security Policy	A password security policy identifies an organization's requirements for strong password creation and security. This prohibits employees from writing down passwords or giving them to other people within our outside of the company.
Employee Monitoring Agreement	The employee monitoring agreement outlines the organization's monitoring activities. Employees should be made aware of cameras and other monitoring devices that are being used. The legality of monitoring varies from region to region. Monitoring must be performed company-wide and only as part of routine monitoring. You cannot target specific employees; this would be grounds for a discrimination lawsuit.
Exit Interview Cooperation Agreement	The exit interview cooperation agreement stipulates the employee's consent to participate in an exit interview. Human Resources conducts the actual exit interview and reminds a soon-to-be ex-employee of the various agreements that they signed when they were initially hired. During this interview any concerns, dissatisfactions, and feedback from the employee is shared. It is essential to maintain a list of termination interview topics to cover with each employee leaving the organization.
Memorandum of Agreement	The Memorandum of Agreement is also known as a Cooperative Agreement. It describes in detail what is required and expected of the employee and employer as a partnership relationship. This document protects both parties and can also lay out milestones and objectives.
Standard Operating	A Standard Operating Procedure (SOP) help employees perform routine and often complex actions. They are step-by-step instructions that help employees work efficiently and improve the quality and uniformity of their work. SOPs also increase

Procedure	compliance with industry standards and regulations.

On the first day of employment, employees should receive the following documents that outline employee expectations and responsibilities:

Document	Description
Security Policy	Employees should receive a written security policy and other security documents related to the employee's position.
Employee Handbook	The employee handbook details the organization's guidelines, expectations, and procedures. The employee handbook can be an important document for the implementation of the security policy, and it should reflect the security posture of the organization. The employee should receive a copy of the employee handbook on the first day of employment. It is customary for the employee to sign a receipt for the employee handbook. In this case, include a one-to-three page summary of items in the handbook for the employee to sign.
Job Description	The job description identifies the responsibilities and tasks assigned to the employee. A job description is the only way to know which qualifications are needed in the new employee. The job description: ▪ Defines the type of experience, training, and expertise you should look for. ▪ Identifies the security access required by the position. ▪ Guides the selection and training process. Protection of the organization's assets should be included in the job description and the employee's job evaluation.

In addition to receiving and signing the above documents, the employee should also sign an inventory of all company assets assigned at the beginning of employment. This inventory, the pre-employment checklist, and employment agreements should be updated anytime the employee gets a promotion, is transfer, or receives new equipment.