IT Onboarding Policy:

Purpose:

The purpose of the onboarding process is to improve employee satisfaction and retention, decrease the time from hire to full productivity, and ensure responsibilities and expectations are clearly defined by providing a formal, systematic approach to creating new hires' accounts, properly configuring devices, and granting appropriate privileges and permissions for network resources in accordance with organizational standards.

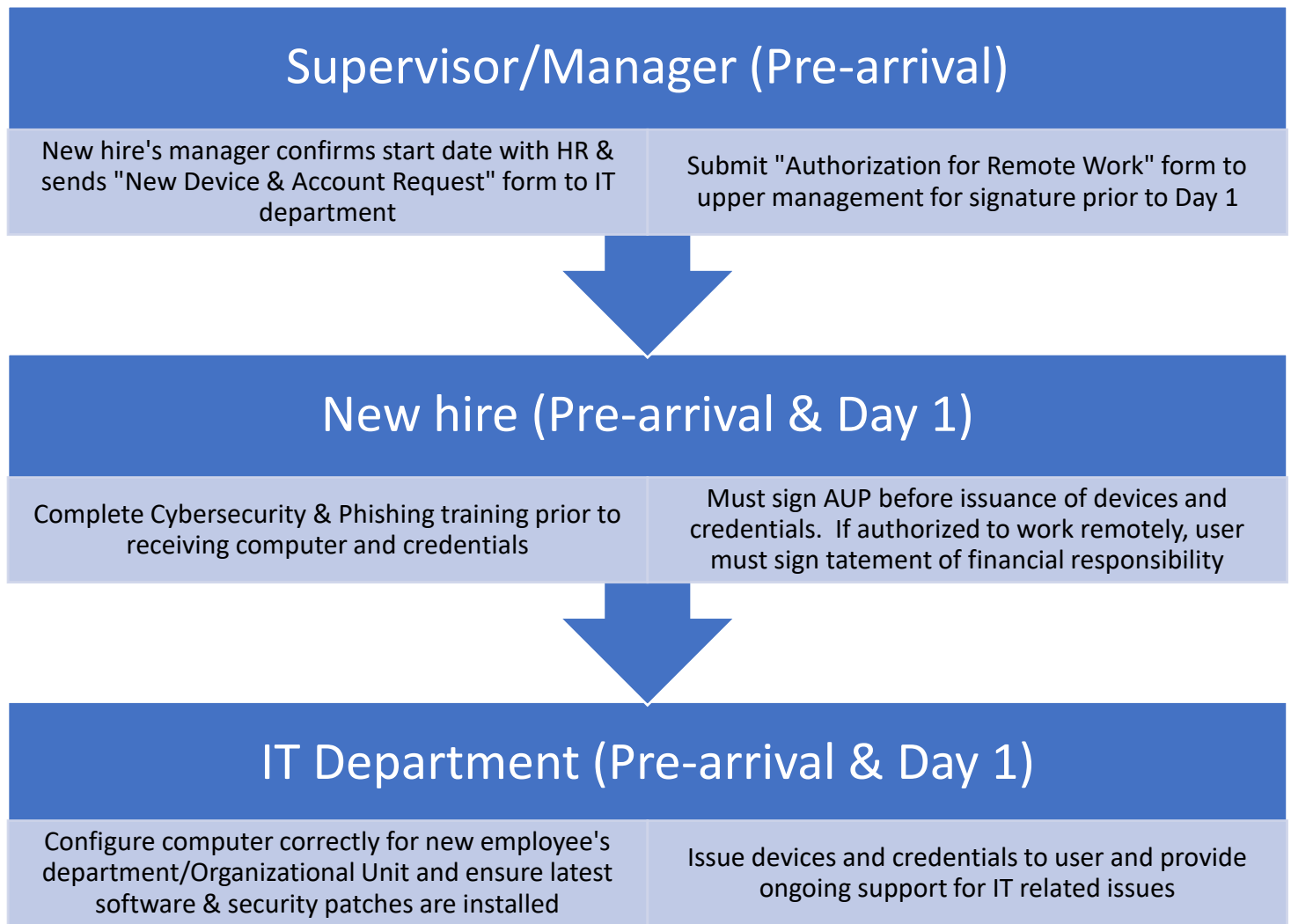**Authorship**:

This policy was written by David Renteria.

Scope:

This policy applies to all new hires – part time and full time – who require access to organizational accounts, devices, and networked resources.

Timeline & Responsibilities:

PERIOD	TASK	ASSIGNED TO	ADDITIONAL INFO
Pre-arrival	Confirm new employee's start date with HR dept and send "New Device & Account Request" to IT dept at least 7 business days before start date	New employee's manager	* "New Device & Account Request" form must include employee's department and any special groups they may be a part of. If new employee requires access to certain resources, please inform IT dept to avoid delays in access. Submit "Authorization for Remote Work" form to management for signatures.
Pre-arrival	Complete cyber-security and phishing training prior to issuing devices and acct info	New employee	https://www.hhs.gov/sites/default/files/hhs-etc/cybersecurity-essentials-training/page55795.html https://www.hhs.gov/sites/default/files/hhs-etc/phishing/index.html *Employee must submit certificate of completion
Pre-arrival	Configure new employee's computer and install latest updates and GPOs	IT dept	
Day 1	Issue user new workstation, grant access to resources, and provide user credentials	IT dept	*New employee must have formal request from management authorizing remote work before remote capabilities & VPN are installed/granted
Day 1	Sign AUP and statement of financial responsibility	New employee	

Onboarding Flow Chart:

Supervisor/Manager (Pre-arrival)

New hire's manager confirms start date with HR & sends "New Device & Account Request" form to IT department	Submit "Authorization for Remote Work" form to upper management for signature prior to Day 1

New hire (Pre-arrival & Day 1)

Complete Cybersecurity & Phishing training prior to receiving computer and credentials	Must sign AUP before issuance of devices and credentials. If authorized to work remotely, user must sign tatement of financial responsibility

IT Department (Pre-arrival & Day 1)

Configure computer correctly for new employee's department/Organizational Unit and ensure latest software & security patches are installed	Issue devices and credentials to user and provide ongoing support for IT related issues

Revision History:

12/18/2023 -- "IT Onboarding Policy" created by David Renteria