Security Policies

Visualize that you are the IT manager/Security Administrator of a mid-sized auto part warehouse with 200 employees and 30 workstation/terminals.

Security Policies such as Acceptable Use Policy, Mandatory Vacations, and Separation of duties: Pick one as the most important and please elaborate the reason.

-Acceptable Use Policy (AUP): is a policy that defines the actions users may perform while accessing systems and networking equipment. The users are not limited to employees; the term can also include venders, contractors, or visitors, each with different privileges. AUPs typically cover all computer use, including mobile devices.
-Mandatory Vacations: Requiring that all employees take vacations. In many fraud schemes, the perpetrator must be present every day in order to continue the fraud or keep it from being exposed. Many organizations require mandatory vacations for all employees to counteract this. For sensitive positions within an organization, an audit of the employees' activities is usually scheduled while they are away on vacation.
-Separation of Duties: The practice of requiring that processes should be divided between two or more individuals. For example, if the duties of the owner and the custodian are performed by a single individual, it could provide that person with total control over all security configurations. It is recommended that these responsibilities be divided so that the system is not vulnerable to the actions performed by a single person.

-CompTIA® Security+ Guide to Network Security Fundamentals, Fifth Edition

The most important policy I would choose is 'Acceptable Use Policy'. This policy governs the actions that users may perform and this can be used to direct and guide toward acceptable behaviors within the work place. Although the other policies are just as equally important, I would choose 'Acceptable Use Policy' because it seems to apply to many different types of professional work environments.

Volatile Data

Software that capture volatile data	Pros & Cons	How to download
Qlik	-Modernize your data and analytics environment with scalable, efficient and real-time data replication that does not impact production system;	www.qlik.com/ Search: qlik streaming change data capture

Software that capture volatile data	Pros & Cons	How to download
Form	-Customize Unique Forms -Gather Actionable Info -Optimize Data Collection	www.form.com Search: data collection software form
Capterra	-Helps organizations find the best software for their needs. -Compare product features and ratings to find the right Electronic Discovery Software for your organization.	www.capterra.com Search: capterra forensic software

-Order of volatility: The sequence of volatile data that must be preserved in a computer forensic investigation.

Locations of data	Sequence to be retrieved
Register, cache peripheral memory	First
Random access memory (RAM)	Second
Network state	Third
Running processes	Fourth

Volatile data is the most difficult type of data to capture. Not only does it have a short “shelf life,” but accessing information at a lower level also can destroy data at higher levels. For example, executing a command to retrieve from a running process can destroy the current contents of registers and RAM. Capturing this volatile information can best be performed by capturing the entire system image, which is a snapshot of the current state of the computer that contains all current settings and data.