Loss Prevention
QUICK REVIEW
DATA SECURITY

DATA STORAGE AND DESTRUCTION

To help prevent unauthorized access to sensitive or private data, follow these best practices:

- Do not allow persons without a badge, key or keypad code into restricted areas even if individuals are known to you. This includes other employees.
- Whenever possible, do not remove any private or nonpublic data from secure storage areas. If you do need to remove items, make sure to follow appropriate security policies.
- Visitors, contractors and vendors in a secure area should have an ID, escort or both.
- Whenever sensitive data is at your workstation, it should be stored in locked cabinets or drawers unless you are there.
- When away from your workstation, you should lock your computer or sign out of the system.
- Keep passwords, keys, ID badges, pass cards, etc. secure or on your person when away from your workstation.
- When destroying confidential, private or nonpublic data, do not simply throw these items into a garbage can. Use a secure form of destruction, such as cross-cut shredders or other means, so as to render the data unrecoverable. Certain types of data may require a certificate of destruction to confirm its destruction.
- For mobile or electronic devices, begin data destruction by manually deleting sensitive items and resetting the device to factory specifications or turn the item in to IT specialists to remove the necessary data.

NOTES: