QUICK REFERENCE

DESTROYING CONFIDENTIAL INFORMATION SECURELY

Objective

Destroy information securely.

Confidential information that hasn't been destroyed properly could fall into the wrong hands.

Target recipient: Everyone

Last update: 2017-06

Recommendations for employees

Paper

- Shred confidential documents or put them in a locked bin if they contain sensitive information.
- Only put documents classified as "public" in a recycling bin.

Email

- Use the **Delete** button to get rid of emails you no longer need.
- Regularly empty your **Deleted Items** folder or turn on the auto delete option.

External hard drives, smartphones, tablets or USB flash drives

- If the file or device is encrypted, delete the file and empty the trash.
- If the file or device isn't encrypted, format the drive and check the **Quick format** box.
- If you plan on giving, selling or throwing away your smartphone or personal tablet, do a reset and completely erase the contents (refer to your user guide or settings).

Recommendations for managers

- Distribute the security measure to all employees.
- Provide employees with locked bins or shredders.
- For storage media that cannot be erased securely or that you want to get rid of, use the services of a data destruction company. You must sign a contract with the company.