How are Apple devices erased?

The iOS devices are typically erased using Cryptographic Erase.

With this method data on device is rendered unusable by overwriting or changing the key used to encrypt or decrypt the data. Blancco 5 Mobile downloads the latest firmware from Apple and then restores this to the device. In this process, the old AES-256 encryption keys are deleted and overwritten by the system. The operating system gets renewed and totally new encrypted file system is created over the old encrypted file system. This encrypted file system replacement makes the recovering of old data totally impossible as there is new AES-256 encrypted file system on top of the old one and the old encryption keys are permanently removed. Overwriting the data is therefore not necessary. Apple's security architecture is based on Advanced Encryption Standard algorithm (AES), a datascrambling system published in 1998 and adopted as a U.S. government standard in 2001. AES is widely regarded as unbreakable. The algorithm is so strong that no computer imaginable for the foreseeable future-even a quantum computer-would be able to crack a truly random 256-bit AES key. The National Security Agency has approved AES-256 for storing top-secret data:
https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

More info about Apple security:
https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf

It is also possible to overwrite the storage after Cryptographic Erase.