FOR IMMEDIATE RELEASE

Waterproof Defender 3000 Flash Drive by Kanguru Provides Top-Notch Data Security For Any Organization

Millis, MA, USA – December 6, 2016 –The waterproof Kanguru Defender 3000™ hardware encrypted flash drive is an ideal data security device for any organization seeking to protect data on the go. **Kanguru Solutions**, a U.S.-based company, designed the powerful flash drive to address the most demanding security standards for government, military and enterprise markets, however, its affordable price makes it ideal for any industry. The rugged alloy housing and epoxy encapsulated cryptographic processor ensures that important information cannot be compromised in any type of environment, helping organizations meet the toughest government data security regulations.

The government-certified **Kanguru Defender 3000** comes with a host of robust features:

- FIPS 140-2 Certification, Level 3
- SuperSpeed USB 3.0
- 256-Bit Hardware Encryption
- Remote Management Ready
- Windows, Mac & Linux Compatibility
- On-Board, Real-Time Anti-Virus Scanning (30-day FREE trial)
- Brute-Force Protection
- Tamper-Proof
- Waterproof
- RSA-Digitally-Signed Secure Firmware
- TAA Compliance

A Secure Alternative to the Cloud

There is simply no safer place to store data than within a locally-stored AES hardware encrypted environment. As organizations consider a variety of options to store and conduct business around the world, companies are realizing that storing data in the cloud could be inadequate at times with service interruptions, as well as a few potential security issues. The hardware encrypted **Kanguru Defender 3000** provides the best security and convenience option, ensuring that the data is secured within the user's possession, backed by robust password protection, and a compilation of tamper-resistant defenses. Users can take their data anywhere and work remotely, all within the confines of the secure environment. Kanguru even offers pre-loaded data services by request. If an organization requires a large staff to operate with specific pre-loaded software or parameters, Kanguru can provide a customized solution to meet those needs.

Remote Management for Advanced Security Environments

For organizations requiring an additional level of security, the Defender 3000 can be remotely managed by the IT security department. **Kanguru Remote Management** enables IT Administrators to manage the device anywhere in the world, send messages to the user, report on the devices whereabouts and customize the settings of each Defender secure drive. In cases where an organization may need to delete or disable the device due to rogue circumstances, Kanguru Remote Management enables an administrator to remotely wipe or disable the device immediately. This advanced management system provides organizations with ideal security and a highly-convenient way to conduct business anywhere.

To learn more about the Kanguru Defender 3000, call Kanguru at **(1) 888-KANGURU** (1-888-526-4878) to talk with a helpful representative, or visit the Kanguru website at **kanguru.com**.

Kanguru provides FIPS 140-2 Certified, TAA compliant, hardware encrypted flash drives, hard drives and solid state drives, as well as fully-integrated remote management security applications, Endpoint Security, and Duplicator products. For more information, visit **kanguru.com**.

FOR MORE INFORMATION, PLEASE CONTACT:

Don Wright, Marketing Manager
Kanguru Solutions
marketing@kanguru.com
(1) 508.376.4245