CARE AND USE OF YOUR RSA SECURID TOKEN

Your new RSA SecurID® token is part of a technology system from RSA, The Security Division of EMC, that protects your organization’s valuable resources. Follow your system administrator’s instructions for using your assigned RSA SecurID token and getting your own Personal Identification Number (PIN). In addition, for your own protection and that of the system, always take the following precautions:

PROTECTING YOURSELF

• Never reveal your PIN to anyone. Do not write it down.
• If you think someone has learned your PIN, notify the security administrator, who will clear the PIN immediately. At your next login you will have to receive or create a new PIN to use.
• Exercise care not to lose your RSA SecurID token or allow it to be stolen. If your token is missing, tell an administrator immediately. The administrator will disable it so that it is useless to unauthorized users.
• Do not let anyone access the system under your identity. (i.e., log in with your PIN and a code from your RSA SecurID token).
• Always follow your system’s standard logoff procedures. Failure to log off properly can create a route into the system that is completely unprotected.

PROTECTING YOUR AUTHENTICATION

While your RSA SecurID token has been designed to comply with strict industry standards, it contains delicate and sophisticated instrumentation and therefore should be handled accordingly:

• Do not immerse your token in liquids, do not expose it to extreme temperatures, and do not put it under pressure or bend it.
• Do not attach or otherwise affix your token directly to devices that generate electromagnetic radiation (EMR), such as mobile phones, phone enabled PDAs and smart phones. At close range (less than 3 inches), these devices can output high levels of EMR that can interfere with the proper operation of electronic equipment, including your token. To be safe, RSA recommends that you carry and store your token separate from your EMR device.