

# Distributed User Support During a Pandemic

## Social Distancing, Business Continuity and Disaster Recovery

### **Characteristics of a Pandemic**

- Officials and experts do not know how long a pandemic could last.
- Communities may be affected in waves that last between six and eight weeks and may continue for up to 18 months.
- State and federal laws may be modified, suspended or enacted in response to a pandemic.
- Healthcare resources will likely be stretched beyond capacity.
- Up to 40% of a workforce may be absent at one time.
- Social and economic disruption is likely.
- If infected, people may be ill for approximately two weeks.
- Susceptibility to the outbreak is universal.

### **Actionable Response to Outbreak**

- Implement SD during a health emergency when extraordinary measures are required to control the spread of disease or infection.
- Decide which social distancing measures, policies, and operational changes make sense to implement.
- Change employee work practices to allow social distancing and continuation of business operations.

RocITSafe™ - Bare-Metal-Boot Virtual System on a Stick is designed from the ground up to provide one of the most secure virtual USB computing platforms ever constructed – the ultimate in secure mobile computing. RocITSafe leverages virtually any PC-based laptop or desktop computer system as the host platform. Then it seamlessly incorporates device management within the RocITSafe guest operating system, supports industry standard software packages and proprietary packages that run within the RocITSafe guest operating system(s) (Windows XP; Windows 7) providing users the flexibility to customize their individual RocITSafe platform according to specific needs or desires without compromising security and data protection within the RocITSafe computing system. RocITSafe supports everyone from the casual user to the sophisticated Super-user.

### **Problem Statement**

One of the most important public health issues our Nation and the world faces is the threat of a global disease outbreak called a pandemic. No one in the world today is fully prepared for a pandemic – but we are better prepared today than we were yesterday - and we will be better prepared tomorrow than we are today.

The world has experienced influenza pandemics three times: as recently as 1968 and 1957 and what has been called the Great Influenza in 1918, a pandemic that killed 40-50 million people worldwide. At some point in our nation's future another virus will emerge with the potential to create a global disease outbreak. History teaches us that everything we do today to prepare for that eventuality will have many lasting benefits for the future. We will realize important advances in healthcare, and we will be better prepared for other types of emergencies.

Adequate planning for a pandemic requires the involvement of every level of our nation, and indeed, the world. The ubiquitous nature of a pandemic compels federal, state and local governments, communities, corporations, families and individuals to learn about, prepare for, and collaborate in efforts to slow, respond to, mitigate, and recover from a potential pandemic. The development, refinement, and exercise of pandemic plans by all stakeholders are critical components of preparedness.

Specifically, when considering the technological challenges that must be addressed during a pandemic, it becomes quite clear that it is exactly these types of events – during the time when people, businesses and government agencies are at their highest risk – provide the greatest opportunities for cyber-thieves and cyber-terrorists to hit the hardest.

## RocITSafe™ - complete data protection on Ultra-mobile platforms

RocITSafe is available today on multiple sizes of FIPS and non-FIPS certified thumb drives as well as FIPS and non-FIPS certified USB spinning hard drives in sizes to over 500GB. RocITSafe creates a highly secure and ultra-mobile container in which the user environment resides including a user-specified OS, user-specific application software, device management tools and Anti-Virus software as well as user-generated data.

By adding CAC/PIV/Smartcard fully integrated login support within RocITSafe, the system has multi-factor authentication, which virtually guarantees your system cannot be compromised through unauthorized access and because of the unique design characteristics of the RocITSafe stack, outside unauthorized access points into the system are eliminated.

### Real Threat – Real Solution

In this worldwide heterogeneous technological environment more data is transmitted in a single hour than the sum total of the entire Library of Congress and then some – a severely under protected network and mobile environment where people are lulled into the misplaced belief that their information is safe and secure. Add to this, that workforces will overnight become remote workers scattered and working in uncontrolled settings that usually are not considered, the result can be devastating.

Business Continuity (BC) and Disaster Recovery (DR) are critical components of any Pandemic plan. With workers scattered remotely both control and support are at best minimal. Yet at these critical times, maintaining continuity and recovery of operations within the organization is vitally important to the long term recoverability after the emergency subsides. Failing to provide support in these two areas can result in loss of important data, loss of productivity and possibly loss of revenue and even disastrous longer-term impact on the organization such as total business failure. A recent statistic quotes 50% of those businesses that suffer major data breaches, data losses due to catastrophic emergencies and organizations that do not have BC and DR plans in place fail within 5 years after the occurrence of such event.



Social distancing (SD), self-shielding, voluntary isolation, and reverse quarantine are all methods that attempt to limit close physical proximity between infected and healthy individuals. They provide individuals with some measure of personal control over their own exposure to a potential pandemic. SD can be instituted voluntarily by individuals or through actions taken by local, state, or government officials such as closure of public office buildings, schools, discontinuance of public transportation, and restrictions on large gatherings or public venues. Additionally, businesses with a

pandemic support plan may institute an (SD) policy for their workforce during a major outbreak. All of these have significant impact on the community and workforce.

### Pandemic Support Solution

RocITSafe combines technologies to provide a standardized method to secure information on Ultra-mobile devices – technology that allows the information to protect itself. RocITSafe technology is highly portable and standards based so can comply with local, state, federal and international data protection standards as they are adopted around the country and around the globe.

The software stack is designed to provide a high degree of flexibility in configuring the systems according to specific user requirements. Specific policies governing Disaster Recovery and Business Continuity within the organization can be included, managed and enforced within the RocITSafe stack.

RocITSafe supports standard methods for connecting to the network including landlines, basic WiFi, WiMax, Mobile Intelligent MiFi hubs, VPN access and others to supports Social Distancing while maintaining smaller functional coherent workgroups which allow the users to lock down an open Internet connection, create a



## Solution Brief: Pandemic Support

highly mobile and secure endpoint to safely connect to critical resources and use a uniform tool set that is easily maintained by small IT organizations before, during and after a major catastrophic event.

Mobile workers and/or students can connect to the secure RocITSafe solution using their ID Cards and a portable CAC/PIV or Smart Card Reader.

### ***About RocITSafe Family: Securing, Enabling, Mobilizing***

The RocITSafe bare-metal-boot (BMB) solutions are best suited to companies that want to virtualize the entire user's desktop, while RocITSafe Pluggable (PG) is better suited to deploying certain applications that the users need all the time, such as a VPN connection or certain desktop applications. PG collaborates with the operating system on the PC, while BMB runs with its own standalone highly secure operating system.

Under central administrative control, both versions can restrict what executables can run within the virtual desktop, and thus prevent data leakage via malware on the host PC.

Absolute Identification's RocITSafe family of products are designed and developed from the core with the highest level of security in mind. Every RocITSafe solution contains a fully integrated and highly secure operating environment that dramatically enhances the ability to protect the user against Cyber-theft.

#### **Headquarters**

5353 Scotts Valley Dr.  
Suite D  
Scotts Valley, CA 95066  
Phone: (831)459-8199  
Toll Free: (888)459-8199  
Fax: (831)480-5886  
[Info@absolute-id.com](mailto:Info@absolute-id.com)

#### **ABID International**

114 France St.  
DDO, Quebec  
Canada, H9A 1K1  
Phone: (831)278-0957  
Fax: (831)515-5256  
[Canada@absolute-id.com](mailto:Canada@absolute-id.com)

#### **ABID Federal**

22 East 35th Place  
Steger, IL 60475  
Phone: (708)755-1583  
Phone: (831)278-0952  
Fax: (831)515-5215  
[Federal@absolute-id.com](mailto:Federal@absolute-id.com)