blancco

Business Continuity & Data Erasure

5 Tips for Uncertain Times

Why Blancco

Blancco is the industry standard in data erasure and mobile device diagnostics software. Our data erasure software provides thousands of organizations the tools they need to enable sustainable data sanitization processes across the widest array of IT assets. By focusing on erasing and reusing assets instead of physically destroying them, organizations can improve their security posture and address corporate social responsibility requirements, while also ensuring compliance with local and global data privacy requirements.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories. All Blancco erasures are verified and certified, resulting in a tamper-proof audit trail.

A global climate of uncertainty brings with it more questions than answers. Based on conversations with existing customers, Blancco addresses five areas of concern to enterprise business continuity teams.

1. Restricted Access for External Vendors and Service Providers

Planned data center and desktop decommissioning projects have historically been done using active engagement onsite by external vendors. New lock-down policies by many global enterprise organizations during crisis situations make this a challenge to operations. To overcome these issues and avoid assets stacking up, Blancco can help advise on best practices for deploying efficient data sanitization processes internally using your own staff. We can also show you how to leverage remote erasure capabilities with a full audit trail. This enables equipment to be released from the facility without risk of data breaches and allows risk-free pickups without unnecessary human interaction.

2. Ensuring Sanitization During Unplanned Reductions of Employees, Consultants and Temporary Staff

In times of hardship, there are often unplanned emergency reductions or changes in an organization's workforce. Company-owned assets (or assets containing sensitive company data) used by individuals leaving the business will need to undergo proper data sanitization with a full audit trail when no longer in use. Remote erasure can remove these concerns by targeting employee equipment and sanitizing data once an employee is no longer using a particular device—without the need for that employee to leave his home environment. This satisfies two major concerns:

- Ensuring that no assets are traveling with sensitive data still on them.
- Removing employee access to sensitive data that could pose an internal security risk. Having a data erasure process for both these scenarios also means meeting ISO 27001 guidelines.

3. Secure Data Sitting with At-Home Workers, Following NIST Security Guidelines

Securing digital data in the home office is of the utmost importance. When the workforce leaves the secure office environment, it is inevitable that more sensitive data than normal will be processed and accessed from less secure remote locations, hence creating an environment where corporate data and personal data may be at risk of data breach. It is important to take best practices to ensure that privacy laws such as the EU GDPR and Personal Data Protection Act are adhered to, even in home office environments. Here are a few tips for securing data in these environments:

- To securely delete files, users can be instructed to actively put files that are no longer necessary in the recycle bin. Using Blancco File Eraser, IT admins can then script remote work computers to securely and automatically erase data in the recycle bin every time the system shuts down.
- Recordings of virtual meetings that can potentially carry retention periods or contain sensitive discussions should be securely erased when no longer required by the user.
- Temporary solutions for file sharing, back-ups and communication could all require active data erasure, especially when data is being saved outside of normal physical and network security of the office. Blancco can advise IT teams on the best ways to address these concerns.
- Under more remote circumstances, you may see increased email traffic containing attachments with sensitive data. Protecting this data is important for security and compliance reasons. Blancco can enable you to automatically target hidden copies of email attachments on endpoints via central deployment to avoid increased risk of data breaches.

The National Institute of Standards and Technology (NIST) advises in its **"Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Special Publication 800-46r2,"** that organizations should:

> ***...store and access only the minimum data necessary.***
>
> Some organizations issue "loaner" devices that are completely wiped before and after the high-risk telework (such as certain foreign travel) is performed. Only the data and authorized applications needed for the telework are loaded onto the loaner device. The loaner devices are used for telework only and may not be connected to the organization's internal networks. The pre-use wiping ensures that the device is clean before any telework is conducted, and the post-use wiping ensures that no telework data remains that could be accessed in the future."

As many employees are temporarily moving to remote work from office environments, many companies also consider BYOD policies as a convenient way to enable employees' access to work.

Remote erasure and automation—combined with centralized auditability—is key to support security initiatives for a remote workforce.

It is very important to ensure corporate data stored in BYOD devices is limited, and any stored data removed once it becomes redundant. NIST 800-46r2 states that "[o]rganizations may find it particularly challenging to address data wiping for BYOD devices. Because the devices are used for both personal and work purposes, it may be necessary to scrub the telework data without affecting the personal data." Blancco File Eraser could be helpful in enabling companies to erase corporate data without touching personal data from BYOD devices.

It's important to also consider remote access servers. As NIST SP 800-46r2 advises, "For portal servers that may temporarily store sensitive user data, wiping such data from the server as soon as it is no longer needed can reduce the potential impact of a compromise of the server."

4. Securing Data in Backup Locations and Disaster Recovery Sites

During crises, businesses often activate back-up workplaces for critical functions. Today, that has become more important than ever, as some corporate locations may be compromised by affected individuals, and operations may need to move elsewhere. For example, if an individual on the trading floor of a bank is found to be infectious, operations (including daily use equipment like desktops/laptops) may move to a backup site to comply with quarantine and sanitization rules. Before moving en masse, devices should be erased to protect against data loss or theft during transport. Likewise, if you have back-up equipment at an alternative location, erase it when you stop using the back-up location. The same is true with disaster recovery sites. When moving data processing and storage to alternate locations, each data migration will require proper data sanitization and an audit trail before that site can be considered securely decommissioned.

5. Sanitizing Temporary Assets When No Longer Needed

Many employees are temporarily moving to remote work from office environments. As part of these moves, many companies are purchasing or renting additional equipment to help facilitate at-home work. Short-term laptop leases, for example, allow employees to work from home if they have desktops at work. Before these devices are returned to the lessor, they must be completely sanitized to remove any sensitive employee, company or customer information. A certificate should be obtained for every erasure to prove compliance with a full audit trail. Additional asset procurement will also need careful assimilation into professional asset management routines, particularly if devices are being shipped back and forth to remote workers or to vendors, putting sensitive data at risk during the chain of custody process. Whether renting or purchasing, remote erasure of these devices is crucial prior to lease or return to the company.

Reducing the need for face-to-face interactions and frequent travel can be important during uncertain times. Remote erasure and automation—combined with centralized auditability—is key to supporting security initiatives for a remote workforce.

Today, mature processes to remotely erase selected files and folders, entire desktops and laptops, as well as servers, SANS and VMs are a natural part of best practice implementations for large enterprises with assets spread around the world.

For more information, please visit our website at www.blancco.com.