



Highlights

- Facilitates greater control over sensitive data by helping you keep your failed media components
 - Helps better manage regulatory compliance to avoid related penalties
 - Helps simplify asset accounting of failed drives as capital IT assets by embedding retention in hardware maintenance support costs
-

Retention for defective media components

Help protect data by keeping failed media components in-house

In the event of a hard disk drive (HDD), solid-state drive (SSD) or flash memory failure, you need to protect one of your most important assets—customer data. Typically, defective media components become the property of the manufacturer and can be refurbished and sold. Though unlikely, it is possible that confidential data could be exposed. As a result, your organization can face penalties from noncompliance with privacy regulations. Many organizations are required to keep defective media components that might contain sensitive data so that the data is under their control.

IBM® Media Support Services for Servers and Storage – media retention is designed to facilitate better control over sensitive data by allowing you to retain HDDs, SSDs and flash memory components for IBM products that are replaced as a result of a service repair action. By planning for media retention before experiencing a failure, you can speed replacement while simplifying asset tracking, depreciation and budget planning. With your HDDs, SSDs or flash memory retained in-house, you can better manage regulatory compliance mandates and proactively resolve the issue of customer data retention.

Enabling enhanced control over data to help protect sensitive information

The media retention service option helps protect sensitive data stored on failed media components that need to be replaced. Rather than having defective media components returned and refurbished as used returnable parts, which can be a security or compliance risk, you can keep the defective HDD, SSD or flash memory on your premises. This way, you can better safeguard the security and privacy of sensitive data without having to purchase the failed media component at its retail price.



Helping you better manage regulatory compliance to avoid related fees

The media retention solution helps you maintain control over the entire chain of custody for regulatory compliance. By helping secure the privacy of highly sensitive information that might be stored on an HDD, SSD or a flash memory card, your business can better manage government regulations, which helps you avoid the fees associated with noncompliance. In addition, you can more easily address privacy concerns in highly sensitive industries such as banking, insurance, medical and the public sector.

Helping simplify asset accounting of replaced drives as capital assets

Instead of dealing with privacy concerns when your HDD, SSD or flash memory needs to be replaced, you can plan for media retention ahead of time to help save money, reduce billing complexity and get your IT systems back up and running more quickly. By embedding media retention in hardware maintenance support, you do not need to track or depreciate the value of the replaced HDD, SSD or flash memory as a capital asset. This helps simplify accounting processes—and can save staff time and effort as the number of HDDs and SSDs increases throughout your organization. Media retention is available as an enhancement to the warranty and maintenance service that distributes the cost of the service over time as an operating expense.

Why IBM?

IBM has deep knowledge of IBM products and is uniquely positioned to provide specialized technical support for your IT environment. IBM has years of expertise in delivering high-quality technical support for complex, multiproduct IT environments. This fixed-price, fixed-scope offering is provided as a hardware maintenance service enhancement—so you can plan your budget more easily.

For more information

To learn more about the media retention offering, please contact your IBM representative or IBM Business Partner, or visit this website:

ibm.com/services/maintenance



© Copyright IBM Corporation 2017

Global Services
Route 100
Somers, NY 10589

Produced in the United States of America
June 2017

IBM, the IBM logo, ibm.com, and Global Technology Services are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



Please Recycle