CYBERARK®

WHITEPAPER

Addressing the Monetary Authority of Singapore Technology Risk Management Guidelines with the CyberArk Identity Security Platform

Table of Contents

Introduction 3

Privileged Accounts Open the Door for Threat Actors 4

CyberArk Identity Security Platform Mitigates Risk 5

Addressing TRM Guidelines with CyberArk Identity Security Solutions 7

Conclusion 14

Introduction

The Monetary Authority of Singapore (MAS) **Technology Risk Management (TRM) Guidelines** is a collection of best practice standards intended to help financial institutions (FIs) strengthen cybersecurity and mitigate risk. TRM Guidelines apply to all financial services companies licensed to do business in Singapore and their service providers including banks, insurance companies, brokers and dealers, credit card companies and investment firms.

The TRM Guidelines provide recommendations for maintaining cyber resiliency and establishing sound and robust technology risk governance and oversight practices. MAS recommends FIs conduct periodic, independent audits to verify compliance with the Guidelines.

MAS revises the guidelines from time to time to keep pace with emerging technologies and shifts in the threat landscape. The latest TRM Guidelines, issued in January 2021, address security issues related to digital transformation. They supersede the June 2013 TRM Guidelines and contain a number of revisions and new recommendations that have arisen from the increased adoption of cloud services, CI/CD practices, DevSecOps methodologies and other advances in financial services information technology.

The TRM Guidelines provide recommendations for maintaining cyber resiliency and establishing sound and robust technology risk governance and oversight practices.

Privileged Accounts Open the Door for Threat Actors

The TRM Guidelines include key requirements related to privileged access management (PAM). Privileged accounts are special accounts like Linux SuperUser/Sudo accounts, Windows administrator accounts, application admin accounts and public cloud admin accounts that system administrators use to manage physical and virtual resources, including systems hosting financial services applications.

Privileged accounts provide powerful access to system commands, files and resources and can be used to exfiltrate financial data, to disrupt IT systems that support financial services and to carry out financial fraud and abuse.

Privileged accounts are inherently difficult for IT organisations to track, manage and secure. They are:

- Built into a variety of systems, databases and applications
- Scattered across a variety of on-premises and cloud infrastructure
- Used by a variety of people—employees, contractors, external support and maintenance vendors and service providers, etc.
- Used by a variety of non-human identities—applications, automation scripts, bots, etc.[1]

With the explosion in human and non-human identities, financial institutions will encounter challenges in boosting their cybersecurity posture. Many financial institutions' information security and IT organisations rely on manual processes to administer privileged account credentials and monitor and control privileged access—a resource-intensive, time-consuming proposition that is fraught with risk. Threat actors can take advantage of weak privileged access management programs to compromise privileged accounts, making it significantly easier to steal or manipulate sensitive data, including financial records, and orchestrate cyber attacks.

[1] Applications, automation scripts, bots, and machines use privileged credentials and secrets to programmatically access enterprise resources and data.

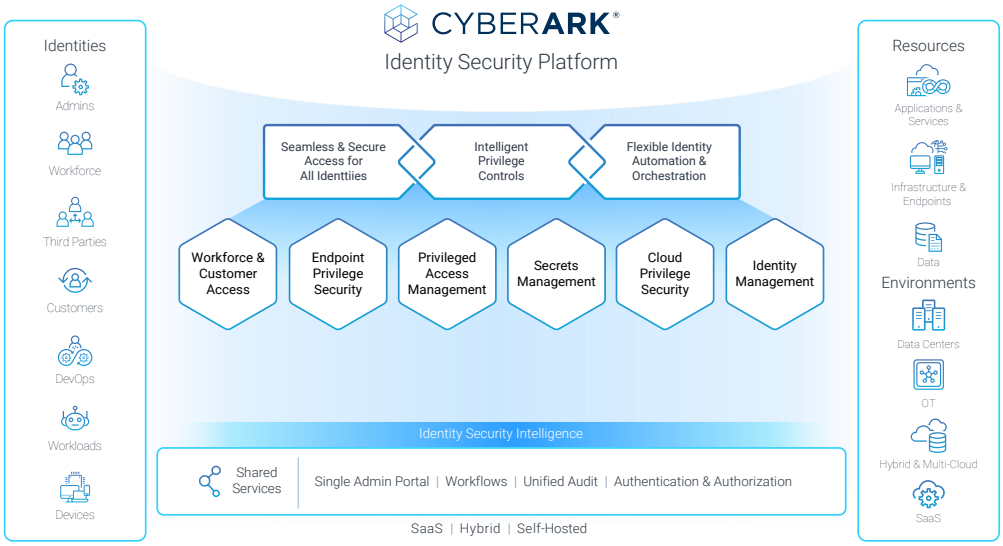
CyberArk Identity Security Platform Mitigates Risk

CyberArk offers a comprehensive, unified Identity Security Platform centered on privileged access management to help FIs increase automation and eliminate inefficient and risk-prone administrative practices. CyberArk privileged access management solutions improve visibility and control and defend against cyber attacks and data breaches.

FIs can use CyberArk Identity Security Platform to help:

- Discover, manage and control all privileged accounts
- Ensure only authorised users have access to privileged accounts
- Isolate, track, monitor and record all privileged access to sensitive servers, databases or virtual machines by internal users and third parties
- Uniquely identify all administrative users and restrict their use of privileged accounts to necessary job functions
- Ensure vendor-supplied default passwords are changed and automate password changes for all privileged accounts
- Eliminate hard-coded credentials, including passwords and encryption keys, from applications, service accounts and scripts without impacting application performance or business flows
- Analyse, detect and alert on anomalous privileged user behaviour to enable quick action by incident response teams
- Provide employees, partners and customers efficient, secure one-click access to cloud, mobile and legacy apps via single sign-on (SSO)
- Implement adaptive multifactor authentication (MFA) for added security for controlling access to corporate applications
- Provision just-in-time privileged access to sensitive resources for external vendors with biometric MFA
- Efficiently onboard users and manage entitlements throughout the employee lifecycle

The CyberArk Identity Security Platform helps organizations enable security in a holistic, unified end-to-end manner focused on six key areas as shown in the following illustration.



Key technologies that help support these areas include:

- **CyberArk Privileged Access Manager**, which provides foundational controls for protecting, controlling and monitoring privileged access across on-premises, cloud and hybrid infrastructure. The solution helps organisations efficiently manage privileged credentials with strong authentication methods, proactively monitor and control privileged account activity, intelligently identify suspicious activity and quickly respond to threats. Financial institutions can self-host CyberArk Privileged Access Manager on-premises or in the cloud, or deploy the solution as a cloud-based service.
- **CyberArk Endpoint Privilege Manager**, which defends Windows, macOS and Linux endpoints against attacks by removing local admin rights from workstations and servers, giving users the minimum set of capabilities needed to perform their jobs, and provides just-in-time (JIT) privilege elevation for remote maintenance and support.
- **CyberArk Vendor Privileged Access Manager**, a SaaS solution that combines Zero Trust access, biometric multifactor authentication and JIT provisioning to secure external vendors that require privileged access to critical internal resources. The solution enables security teams to provide external vendors with only the access they need. Vendor PAM fully integrates with the CyberArk Privileged Access Manager solution for full audit, session isolation and remediation capabilities.
- **CyberArk Cloud Entitlements Manager**, a SaaS solution that reduces risk by implementing least privilege across cloud environments and boosting cloud privilege security. From a centralised dashboard, Cloud Entitlements Manager provides visibility and control of identity and access management (IAM) permissions across an organisation's cloud estate (e.g., AWS, Microsoft Azure, Google Cloud admin accounts). Cloud Entitlements Manager leverages artificial intelligence to detect and remediate risky permissions, helping organisations strategically reduce risk without disrupting necessary access for cloud operations.
- **CyberArk Conjur Secrets Manager Enterprise**, which enables organisations to centrally secure and manage secrets and credentials used by the broadest range of applications, including internally developed applications; commercial off-the-shelf software; robotic process automation platforms; and CI/CD tools running in private, public, hybrid and containerized environments.
- **CyberArk Identity**, a SaaS-delivered suite of services designed to help organisations securely manage identity and access for their employees, partners and customers. CyberArk Identity helps organisations improve employee productivity, enhance customer and partner experiences, and reduce the risk of weak or default passwords—the primary cause of security breaches. The CyberArk Identity suite includes all fundamental pillars of IAM—SSO, adaptive MFA, identity lifecycle management and user behaviour analytics.

Addressing TRM Guidelines with CyberArk Identity Security Solutions

FIs can use CyberArk Identity Security solutions to satisfy a variety of MAS TRM Guidelines as detailed in the table below.

Section	Guideline	CyberArk Solution
4 Technology Risk Management		
4.1 Risk Management Framework		
4.1.2	Effective risk management practices and internal controls should be instituted to achieve data confidentiality and integrity, system security and reliability, as well as stability and resilience in its IT operating environment.	CyberArk Identity Security Platform help financial institutions mitigate risk by securing human and non-human identities across on-premises, cloud and hybrid environments. PAM solutions help FI security and IT teams monitor, manage and control access to critical applications, resources and data from inside or outside the enterprise, helping protect data confidentiality and integrity and defend systems against malicious attacks. The CyberArk solutions include a hardened tamper-resistant Digital Vault for safely storing sensitive data such as credentials and log files.
6 Software Application Development and Management		
6.3 DevSecOps Management		
6.3.2	The FI should implement adequate security measures and enforce segregation of duties for the software development, testing and release functions in its DevSecOps processes.	CyberArk Secrets Management solutions let FIs development, test, operations and security teams efficiently control and manage the credentials used by a variety of applications and systems. The solution removes hard-coded credentials from applications and scripts, centralises credential storage and administration, and automatically rotates credentials based on policy without modifying code, restarting applications or disrupting business-critical services.
6.3 DevSecOps Management		
6.4.4	Security standards for designing and developing secure APIs should be established. The standards should include the measures to protect the API keys or access tokens, which are used to authorise access to APIs to exchange confidential data. A reasonable timeframe should be defined and enforced for access token expiration to reduce the risk of unauthorised access.	CyberArk PAM solutions provide comprehensive secrets management for privileged credentials such as API keys, certificates, passwords, SSH keys and tokens. Secrets are securely managed and automatically rotated based on policy.

Section	Guideline	CyberArk Solution
6.4.5	Strong encryption standards and key management controls should be adopted to secure transmission of sensitive data through APIs.	CyberArk PAM solutions supports strong encryption standards and provides extensive API key management controls.
7 IT Service Management		
7.7 Incident Management		
7.7.4	The FI should configure system events or alerts to provide an early indication of issues that may affect its IT systems' performance and security. System events or alerts should be actively monitored so that prompt measures can be taken to address the issues early.	CyberArk Privileged Access Manager applies a complex combination of statistical and deterministic algorithms to automatically identify malicious privileged access activity. CyberArk Identity Security Intelligence, a shared service of the Identity Security Platform, uses AI and Machine Learning to collect, analyse and visualise user behaviour and threat data in real time for both workforce and privileged identities.
8 IT Reslience		
8.1 System Availability		
8.1.1	Maintaining system availability is crucial in achieving confidence and trust in the FI's operational capabilities. IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs.	FIs can deploy the CyberArk Digital Vault and other critical self-hosted CyberArk components in high availability configurations to optimize uptime.
9 Access Control		
9.1 User Access Management		
9.1.1	The principles of "never alone," "segregation of duties" and "least privilege" should be applied when granting staff access to information assets so that no one person has access to perform sensitive system functions. Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers.	CyberArk Identity provides comprehensive identity lifecycle management and identity and access management functionality to facilitate role-based access controls and segregation of duties. The solution supports the never alone principle with dual control workflows, requiring two approvers (e.g., a manager and a supervisor) to authorise access rights. CyberArk Endpoint Privilege Manager supports the principle of least privilege by removing standing admin rights from workstations and servers and providing just-in-time elevation for maintenance. CyberArk Privileged Access Manager provides foundational controls for protecting, controlling and monitoring access to privileged users such as system administrators. Dual control workflows can be configured for all access to privileged accounts. Meanwhile, just-in-time CyberArk PAM and Cloud Privilege Security solutions implement least privileged access across AWS, Azure and Google Cloud admin accounts by detecting and removing excessive permissions. Necessary access is protected and monitored for both standing access (with PAM vaulting and isolation) and federated access (using just-in-time elevation).

Section	Guideline	CyberArk Solution
9.1.2	The financial institution should establish a user access management process to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner.	CyberArk Identity provides complete identity lifecycle management with self-service request capabilities for end users and automated approval workflows to minimise helpdesk involvement.
9.1.3	For proper accountability, the financial institution should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes.	CyberArk Privileged Access Manager automatically maintains an audit trail of all privileged session activity in the secure Digital Vault. CyberArk Identity includes logging and reporting functionality for tracking user access and user management activities and for supporting audits and investigations. The Secure Web Sessions capabilities in CyberArk Identity also record access to web applications, with continuous authentication to validate access.
9.1.4	The financial institution should establish a password policy and a process to enforce strong password controls for users' access to IT systems.	CyberArk PAM allows organizations to automatically rotate shared account credentials according to organizational policy, allowing customization of controls like length, age, history, complexity, etc. For workforce users, CyberArk Identity supports strong password controls (length, age, history, complexity, etc.) and includes a password generator for end users.
9.1.5	Multifactor authentication should be implemented for users with access to sensitive system functions to safeguard the systems and data from unauthorised access.	CyberArk Identity supports adaptive MFA to protect systems against unauthorised access. The solution supports a variety of authentication methods and authenticators including passwordless authentication. CyberArk Privileged Access Manager also supports MFA through SAML or RADIUS authentication for securing access to privileged accounts. CyberArk Vendor Privileged Access Manager provides biometric MFA for third-party vendor access to both privileged accounts and web applications.
9.1.6	The FI should ensure appropriate parties, such as information asset owners, to perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as inappropriate access rights. Exceptions noted from the user access review should be resolved as soon as practicable.	CyberArk Privileged Access Manager provides out-of-the-box reports such as entitlement reports to help in the user access review. CyberArk Identity supports access certification campaigns to periodically review and validate user access privileges. CyberArk Cloud Entitlements Manager continuously detects excessive permissions and hidden admin rights in public cloud environments. The service also provides remediation actions to remove excessive permissions and create safer policies.

Section	Guideline	CyberArk Solution
9.1.7	Users should only be granted access rights on a need-to-use basis. Access rights that are no longer needed as a result of a change in a user's job responsibilities or employment status (e.g., transfer or termination of employment) should be revoked or disabled promptly.	CyberArk Identity certification campaigns support automatic closed-loop remediation and admin-invoked remediation to revoke access privileges and avoid orphaned or over-provisioned accounts.
9.2 Privileged Access Management		
9.2.1	Users granted privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment. Access to privileged accounts should only be granted on a need-to-use basis; activities of these accounts should be logged and reviewed as part of the FI's ongoing monitoring.	CyberArk Privileged Access Manager provides foundational controls for protecting, controlling and monitoring access to privileged accounts. FIs can use the solution to: • Safely store privileged account credentials in a tamper-proof Digital Vault • Automatically rotate and update credentials based on policy • Tightly control access to privileged accounts with approval workflows and IT Service Management/Ticketing system integrations • Authenticate users and isolate privileged sessions • Closely monitor and track privileged account activity • Intelligently identify suspicious behaviour
9.2.2	System and service accounts are used by operating systems, applications and databases to interact or access other systems' resources. The FI should establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.	CyberArk Privileged Access Manager intelligently identifies anomalous behaviour, automatically detecting potential data breaches and security incidents. Alerts and automated remediation actions (i.e., termination of suspicious privileged sessions) are also supported.
9.3 Remote Access Management		
9.3.1	Remote access allows users to connect to the financial institution's internal network via an external network to access the FI's data and systems, such as emails and business applications. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multifactor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment.	CyberArk Identity supports adaptive MFA for remote access. The solution supports a variety of authentication methods and authenticators, including passwordless authentication, and supports encrypted communications to defend against eavesdropping and data leakage. CyberArk Privileged Access Manager supports MFA for remote access to privileged accounts. The solution isolates privileged sessions and supports secure protocols like SSH and TLS to prevent data leakage. CyberArk Vendor Privileged Access Manager provides biometric authentication and JIT provisioning for third-party IT support vendors or other service providers that require remote privileged access. The solution supports encrypted communications to defend against eavesdropping and data leakage.

Section	Guideline	CyberArk Solution
10.0 Cryptography		
10.1 Cryptographic Algorithm and protocol		
10.1.2	The financial institution should adopt cryptographic algorithms from well-established international standards. The FI should also select an appropriate algorithm and encryption key length that meets its security objectives and requirements.	Passwords and SSH keys are stored using CyberArk's patented, ICSA-certified Digital Vault, which employs multiple built-in layers of security to protect privileged credentials. Audit and security logs are also stored in the Digital Vault and are protected using FIPS 140-2-compliant AES-256 encryption algorithms.
10.2 Cryptographic Key Management		
10.2.1	Cryptographic key management policy, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiration should be established.	With CyberArk, FIs can institute policies to automatically rotate and update keys. Optional integration with Hardware Secure Modules (HSMs) provide an additional level of private key protection and strong entropy for key generation.
10.2.2	The FI should ensure cryptographic keys are securely generated and protected from unauthorised disclosure. Any cryptographic key or sensitive data used to generate or derive the keys should be also be protected or securely destroyed after the key is generated.	Passwords and SSH keys are stored using CyberArk's patented, ICSA certified Digital Vault, which employs multiple built-in layers of security to protect privileged credentials.
10.2.3	The FI should determine the appropriate lifespan of each cryptographic key based on factors such as the sensitivity of the data, the criticality of the system to be protected, and the threats and risks that the data or system may be exposed to. The cryptographic key should be securely replaced before it expires at the end of its lifespan.	Financial institutions can rotate and update keys automatically based on policy.
10.2.4	To protect sensitive cryptographic keys, the FI should manage, process and store such keys in hardened and tamper resistant systems (e.g., by using a hardware security module).	The CyberArk Digital vault is hardened and tamper resistant and supports hardware security modules. The CyberArk Digital Vault also offers optional integration with leading Hardware Security Modules via out-of-the-box integrations.
10.2.5	When sensitive cryptographic keys need to be transmitted, the FI should ensure these keys are not exposed during transmission. The keys should be distributed to the intended recipient via an out-of-band channel or other secure means to minimise the risk of interception.	Cryptographic keys are never exposed during transmission.

Section	Guideline	CyberArk Solution
11 Data and Infrastructure Security		
11.3 System Security		
11.3.3	Endpoint protection, which includes but is not limited to behavioural-based and signature-based solutions, should be implemented to protect the FI from malware infection and address common delivery channels of malware, such as malicious links, websites, email attachments or infected removable storage media.	CyberArk Endpoint Privilege Manager protects against malware by tightly controlling how applications run—allowing trusted applications to run normally, blocking malicious software and forcing unknown applications to run in a restricted mode.
11.3.5	To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner and proactively monitor systems, including endpoint systems, processes for anomalies and suspicious activities.	CyberArk Endpoint Privilege Manager integrates with external threat intelligence and EDR systems to automatically detect and remediate suspicious activity.
11.3.6	Security measures, such as application allowlisting, should be implemented to ensure only authorised software is allowed to be installed on the financial institution's systems.	CyberArk Endpoint Privilege Manager supports application allowlisting, as well as denylisting and greylisting.
11.4 Virtualisation Security		
11.4.2	Strong access controls should be implemented to restrict administrative access to the hypervisor and host operating system, as both control the guest operating systems and other components in the virtual environment.	FIs can use CyberArk Privileged Access Manager to restrict administrative access to a hypervisor (e.g., VMware ESXi) and host operating system.
12 Cyber Security Operations		
12.1 Cyber Threat Intelligence and Information Sharing		
12.1.1	To maintain good cyber situational awareness, the FI should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's business and IT environment. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities.	CyberArk Privileged Access Manager threat analytics intelligently identifies anomalous behaviour, automatically detecting potential data breaches and security incidents. CyberArk Identity Security Intelligence, a shared service of the Identity Security Platform, uses AI and machine learning to collect, analyse and visualise user behaviour and threat data in real time for both workforce and privileged identities. Security Operations Center (SOC) teams can consume alerts and threat intelligence data in both the CyberArk UI or their SIEM solution via event forwarding.

Section	Guideline	CyberArk Solution
12.2 Cyber Event Monitoring and Detection		
12.2.2	A process to collect, process, review and retain system logs should be established to facilitate the FI's security monitoring operations. These logs should be protected against unauthorised access.	CyberArk Privileged Access Manager automatically maintains an audit trail of all privileged session activity in the secure Digital Vault. Detailed audit and security logs are created and protected with AES-256 cryptographic storage in a tamper-proof digital vault that is FIPS 140-2 compliant. CyberArk Identity includes logging and reporting functionality for tracking user access and user management activities, and for supporting audits and investigations.
12.2.4	The FI should consider applying user behavioural analytics to enhance the effectiveness of security monitoring. User behavioural analytics might include the use of machine learning algorithms in real time to analyse system logs, establish a baseline of normal user activities and identify suspicious or anomalous behaviours.	CyberArk Privileged Access Manager threat analytics intelligently identifies anomalous behaviour, automatically detecting potential data breaches and security incidents. CyberArk Identity user behaviour analytics uses AI and Machine Learning to collect, analyse and visualise user behaviour and threat data in real time.
14 Online Financial Services		
14.2 Customer Authentication and Transaction Signing		
14.2.1	Multifactor authentication should be deployed at login for online financial services to secure the customer authentication process. Multifactor authentication can be based on two or more of the following factors: what you know (e.g., personal identification number or password), what you have (e.g., one-time password (OTP) generator) and who you are (e.g., biometrics).	FIs can use CyberArk Identity to provide multi-factor authentication for customer-facing applications such as online banking. The solution supports a variety of authentication methods including passwordless authentication.
14.2.4	Besides login and transaction signing for high-risk activities, the FI may implement appropriate risk-based or adaptive authentication that presents customers with authentication options that are commensurate with the risk level of the transaction and sensitivity of the data.	With CyberArk Identity, FIs can enforce MFA challenges based on contextual information and behavioural signals.

Conclusion

CyberArk Identity Security solutions can help FIs improve TRM compliance, satisfy auditors and reduce cyber risk by automating administrative practices, improving visibility and control, and defending critical financial services applications and systems against malicious attacks, data theft, fraud and abuse. CyberArk is the established leader in privileged access management, trusted by more than 7,500 customers, including more than half of the Fortune 500.

To learn more about how the CyberArk Identity Security Platform can help your company strengthen security controls, improve TRM compliance and streamline audits **schedule a demo**.

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®

©Copyright 2022 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S., 10.22 Doc. TSK-2362 (TSK-2171)

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.