Comply with the latest SEBI Advisory regarding Remote Access and Telecommuting

Last Updated: 03 February, 2021

Copyright © 2021, Accops Systems Private Limited. All Rights Reserved.

Copyright © 2021, Accops Systems Private Limited. All Rights Reserved.

The information contained in this document represents the current view of Accops Systems Private Limited on the issues discussed as of the date of publication. Because Accops Systems Private Limited must respond to changing market conditions, it should not be interpreted as a commitment on the part of Accops Systems Private Limited. Accops Systems Private Limited cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. ACCOPS SYSTEM PRIVATE LIMITED MAKES NO WARRANTIES, EXPRESSED OR IMPLIED IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the explicit written permission of Accops Systems Private Limited.

Contact Accops Systems Private Limited.

Email: info@accops.com

Call: +91 (0)20 6719 0123

Banking Industry and Remote Work Challenges

SEBI had issued an advisory regarding Remote Access and Telecommuting (Circular No.: NSDL/POLICY/2020/0143, dated October 30, 2020). The SEBI advisory refers to several circulars from SEBI, NSDL, NCIIPC. SEBI advises depository participants on the matter of Remote Access and Telecommuting, as mentioned in the table below.

Accops provides comprehensive zero trust-based secure remote work solutions with all features needed for seamless compliance with the latest guidelines provided by SEBI Advisory. The below table shows how organizations can achieve compliance using Accops solutions:

	SEBI Advisory	Accops Solution/Response.
1	Ensure proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection.	Accops HySecure, an Application Access Gateway allows workforce to safely log in to corporate applications and desktops, and access private applications they need to be efficient and productive. The Layer 4 to Layer 7 application tunnel-based technology creates a zero-trust based access while creating a software defined perimeter (SDP) bringing together performance, management, and security required for enterprise remote access.
2	For implementation of the concept of trusted machine as end users, categorize the machines as official desktops / laptops and accordingly the same may be configured to ensure implementation of solution stack considering the requirements of authorized access. Official devices shall have appropriate security measures to ensure that the configuration is not tampered with. Participants shall ensure that internet connectivity provided on all official devices shall not be used for any	Accops Management Server allows controlled onboarding of devices and users based on profiles by an approved authority in the organization. For example, corporate issued laptop/tablet/desktop to employee, BYOD, vendor issued laptop/tablet/desktop, similar devices issued to contractors. Furthermore, users may have different personas based on roles that they perform. Accops solution will ensure that only whitelisted applications (LoB, Corporate) are visible to a specific persona on an enterprise-approved device(s). These device

Copyright © 2021, Accops Systems Private Limited. All Rights Reserved.

	purpose other than the use of remote access to data centre resources.	approvals are based on the hardware signature of the device, such as CPU ID, motherboard ID, HDD ID and many more. Use of internet at the end user device can be controlled through the Accops agent running on the endpoint with whitelisted URLs only.
3	If personal devices (BYOD) are allowed for general functions, then appropriate guidelines should be issued to indicate positive and negative list of applications that are permitted on such devices. Further, these devices should be subject to periodic audit.	The appropriate authority within the organization should formulate application restriction policies meant for BYOD in terms of application whitelisting. Such policies can be enforced through Accops solutions for BYOD. The Accops Reporting Server provides data on user profiles, application access patterns and host of other data for audit purposes.
4	Implement the various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder's claimed identity.	Accops solutions enable organizations implement strong authentication with its integrated MFA, which uses multiple token options like SMS, email, mobile app or biometrics to ensure strict verification of a user's claimed identity before providing access to corporate applications and data. It also checks device authenticity along with 2FA which makes it a complete MFA solution that thoroughly verifies account holders' identity.
5	Ensure that the trusted machine is the only client permitted to access the data centre resources. The Participants shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.	Accops follows Zero Trust Architecture principles. Accops verifies user and device signatures based on multiple parameters (more than 20) like MAC address, WAN/IP address, geolocation, firewall status, antivirus status, CPU ID, motherboard ID etc. Based on the device and user control, a user on a specific device may be denied access, allowed access or further multi-factor authentication can be enforced. Such policies formulated by the appropriate authority can be enforced through the Accops Management Server. It also pushes restrictive policies to the endpoints where Accops agent is running.
6	Explore a mechanism for ensuring that the employee using remote access solution is	With Accops' facial recognition and authentication features, organizations can

Copyright © 2021, Accops Systems Private Limited. All Rights Reserved.

	indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video-recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. Participants shall implement short session timeouts for better security. Towards this end, it is suggested that the Participants may consider running a mandatory monitor on the device that executes: a. At random intervals takes a picture with the webcam and uploads the same to the Participant's server, b. At random intervals pops up and prompts biometric authentication with a timeout period of a few seconds. If there is a timeout, this is flagged on the Participants server as a security event.	ensure that the employee using remote access solution is indeed the same person to whom access has been granted and not any other unauthorized user. Accops provides organizations with the ability to periodically scan user's face and ensures that there is no chance of identity thefts or credential sharing. The frequency of facial authentication and session time-out can be defined through policies. Accops biometric authentication system also works on the same concept. User's fingerprint scanning is done at the time of login and periodically thereafter, as and when the authentication is timed out. In both methods, security logs are generated to the server and available for audit.
7	Ensure that appropriate risk mitigation mechanisms are put in place whenever remote access of data centre resources is permitted for service providers.	With Accops solution, enterprises can govern the business data and restrict access to managed/approved devices only. While user authentication is secured by 2FA/OTP, endpoint device authentication and authorization will be managed by Accops endpoint security policy which is based on non-spoofable device signature ID like CPU ID, Motherboard ID, HDD ID. This ensures that even if a user has access to User ID, password and 2FA/OTP, he/she still uses only enterprise-approved devices.
8	Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the Participants shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.	Accops Management Server, through its Zero Trust-based contextual, role-based access engine continuously looks for patterns of any abnormal access. In case of any abnormalities, endpoint details will be captured and sent to quarantine profile and a notification is to admin about the unusual access and the login failure of user.

Copyright © 2021, Accops Systems Private Limited. All Rights Reserved.

		However, if the user is genuine, user shall still get his device approved from administrator and attempt to login again. Also, Accops facial recognition will easily identify shoulder-surfing and immediately disconnect users from the session.
9	Ensure that the backup, restore and archival functions work seamlessly, particularly if the users have been provided remote access to internal systems.	Accops automates backup restore and archival of its own components. It also provides proper port access to all endpoint machines and ensures proper, seamless functioning of backup restore and archival functions, while following and complying with the enterprise policy.
10	Exercise sound judgement and discretion while applying patches to existing hardware and software and apply only those patches which were necessary and applicable.	Accops helps organizations apply all critical security patches to existing hardware, software, and other mission critical applications, to all endpoints regardless of location, in a timely manner, from a central location and ensure that all devices remain compliant.
11	The Security Operations Centre (SOC) engine has to be periodically monitored and logs analyzed from a remote location. Alerts and alarms generated should also be analyzed and appropriate decisions should be taken to address the security concerns. The security controls implemented for the Remote Access requirements need to be integrated with the SOC Engine and should become a part of the overall monitoring of the security posture.	Accops solution easily integrates with the existing Security Operations Centre engine and provides the required logs to be monitored by all leading SIEM (Security Information & Event Management) servers.
12	Update its incidence response plan in view of the current pandemic.	Does not appertain to Accops or other IT solution providers.
13	Implement cyber security advisories received from SEBI, MII, CERT-IN and NCIIPC on a regular basis.	Accops provides 100% Make-in-India products and solutions which comply with all cyber security advisories of SEBI, MII, CERToIN and NCIIPC. Accops will continue to incorporate/implement all applicable future

Copyright © 2021, Accops Systems Private Limited. All Rights Reserved.

		advisories received from SEBI, MII, CERT-IN and NCIIPC etc on a timely basis.
14	Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness.	The policies as defined by the appropriate authority in the organization and implemented through Accops Solution shall prevail at all times.

With Accops solutions, organizations can easily ensure that all the aforementioned pointers remain a part of Standard Operating Procedures post Covid-19 situation for enhanced network security and data privacy.

To know more details on our products and solutions, visit our website www.accops.com or send us an e-mail at sales@accops.com to get in touch with our experts.

Accops, HyWorks, HyDesk, HyID, HyLite, HySecure and HyLabs are registered trademarks of Accops Systems Pvt. Ltd. Other names may be trademarks of their respective owners. Accops has the right to change, modify, transfer or otherwise revise the publication without notice.

Tel: India +91 (0)20-6719 0123

Email: sales@accops.com | Web: www.accops.com

Copyright © 2021, Accops Systems Private Limited. All Rights Reserved.