

WORKPLACE TECHNOLOGY REINTEGRATION

When reintegrating technology into the physical workplace, it is important that devices are sterilized—not only from cyber viruses but also airborne viruses like COVID-19.

ESD's Technology Reintegration Guide provides our clients with recommendations for returning technology to the work environment.



STRATEGY & PLANNING



REINTEGRATION PLAN

- ❑ Identify a business leader responsible for developing your workforce reintegration or return-to-work plan.
- ❑ Include a member of your IT Team or hire a Technology Consultant to provide support and guidance for IT Systems related to the return-to-work plan.
- ❑ Ensure the reintegration or return-to-work plan includes the best practices identified for technology.

WORKPLACE MANAGEMENT

- ❑ Implement office space and resource management solutions that help with floor plan mapping, identification of points of interests and consumable such as sanitation supplies.
- ❑ Implement solutions to help with dynamic seat allocation and scenario planning in order to maintain physical distancing guidelines as well as creating seating strategies during staggered re-entry and post return.
- ❑ Deploy touchless visitor management solutions to enable seamless check-in procedures and experiences (automate Wi-Fi passcode generation, health and safety procedures, health and travel declaration forms, etc.).
- ❑ Implement space booking solutions with mobile applications and resource management integration/plug in tools to streamline remote reservation, increase available space visibility, minimize physical collision and touchpoints.



ENTERPRISE TECHNOLOGY



EQUIPMENT SANITATION

- ❑ Use a lint-free cloth, such as a screen wipe or a cloth made from microfiber.
- ❑ Avoid excessive wiping and submerging item in cleanser to avoid damage.
- ❑ Unplug all external power sources and cables.
- ❑ Do not use aerosol sprays, bleach or abrasive cleaners.
- ❑ Ensure moisture does not get into any openings.
- ❑ Never spray cleaner directly on an item.

Approved COVID-19 disinfectants safe for computers, accessories and electronics¹:

- ❑ Isopropyl alcohol (IPA) solution 70% or less
- ❑ PDI Sani-Cloth® Plus
- ❑ Covidien™ Alcohol Prep pads
- ❑ CaviWipes™
- ❑ Clorox Healthcare® Bleach Germicidal Wipes (Macs should not be cleaned with clorox wipes²)
- ❑ Total Solutions® Disinfectant Wipes



COMPUTER HEALTH CHECK

- ❑ Establish a test network if possible before connecting to the corporate production network.
- ❑ Perform a virus scan for malware on all devices before allowing any device to connect to the corporate production network including wired and wireless networks.
- ❑ Visually identify if suspicious files are located in recycle, trash, and download folders.
- ❑ Visually identify if any non-corporate licensed software has recently been added within the remote work time period.
- ❑ Implement a remote computer support software solution to enable IT to be able to remotely connect to user PCs to provide enhanced support capabilities as well as to perform the above steps prior to bringing them back into the corporate network environment.

NETWORK HEALTH CHECK

- ❑ Invest in Cybersecurity analysis and threat tools such as Vulnerability Assessment Platforms and Advance Threat Protection Tools. At a minimum, have a Cybersecurity Vulnerability Assessment with internal and external penetration tests performed by a qualified cybersecurity consultant.
- ❑ Maintain all updates for software and verify all devices are up to date with current patches and security updates before connecting to the corporate production network.
- ❑ Perform a backup of all corporate production systems to establish a point of recovery before connecting devices to the corporate production network.



BUILDING TECHNOLOGY



AUDIO VISUAL

- ❑ Leverage existing digital signage to continue flow of corporate communication and employee awareness.
- ❑ Evaluate existing conference room technology and infrastructure to help enable deployment of Unified Communication & Collaboration (UCC) platforms if not currently present. Include in-room PC, wireless presentation device, USB cameras, microphones, etc.
- ❑ Review of home office audio visual infrastructure for senior leadership. Include docking stations, 2nd monitors, microphone/speaker and Bluetooth headset.



SECURITY

- ❑ Implement a temperature scanning program for all people entering your space with a fever notification protocol; potentially integrated with your access control system. Program should identify:
 - ❑ A show of 'Duty of Care'
 - ❑ Reliable testing to ensure detection
 - ❑ Liability concerns
 - ❑ Impact to operations
- ❑ Incorporate frictionless access control devices into your access control system to minimize common touch-points.

WIRELESS NETWORK

- ❑ Consider a spectrum analysis of wireless network for signal strength, signal to noise ratios, co-channel interference and sources of signal interference
- ❑ Ensure that appropriate wireless security measures have been implemented such as:
 - ❑ Disable Broadcast SSID (Set Service Identification)
 - ❑ Implement data protection and network access control measures such as WPA2 or WPA2-PSK
 - ❑ Segregate wireless traffic streams using VPNs



ESD's Technology Consulting Team is here to assist with developing your requirements and programs, provide support for reintegrating technology into the work environment and determining the right audio visual, security and wireless upgrades.

For more information and to contact one of our Technical Consultants, please visit www.esdglobal.com/COVID-19.

RESOURCES

- 1 <https://support.microsoft.com/en-us/help/4023504/surface-clean-and-care-for-your-surface>
- 2 <https://support.apple.com/en-us/HT204172>

tech-knowledge /tek'näləj/ noun

ESD's news source for digital solutions in the built environment.