Uptime Institute
INTELLIGENCE

RISK & RESILIENCY

UI Intelligence report 37 v2

Pandemic planning and response: A guide for critical infrastructure

Authors
Uptime Institute Intelligence team

This advisory report has been produced by Uptime Institute, with the assistance of clients and members, to help operators of critical infrastructure facilities prepare for, and respond to, the impact of the novel coronavirus that causes COVID-19. The steps discussed in this report will also help operators develop strategies and procedures for future pandemics.

This report updates and replaces Uptime Institute report 37 v1, ***COVID-19: Minimizing critical facility risk****.*

30-45 minutes to read

UII-37 v2.0 published May 12, 2020 last updated May 12, 2020

This Uptime Institute Intelligence report includes:

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

INTRODUCTION

During a pandemic, operators of mission-critical digital infrastructure facilities face particular challenges due to the high risk of unavailability of key staff through illness or quarantine, along with other events and measures (e.g., lockdowns, facility contamination) that might affect the ability of the operator to maintain continuous availability of IT services.

Fortunately, preparedness is in the industry's DNA; while many operators did not plan specifically for a global health emergency, thanks to their focus on performance, efficiency and reliability — tested through prior experience with power blackouts, wildfire, adverse weather and other potentially disruptive events — most data centers owner/operators have contingency plans in place that can be adapted to the challenges of a pandemic.

The main priorities for those plans are the health and safety of staff, partners and customers; business continuity; and compliance with the guidelines and regulations issued by public health and government agencies.

This report reviews the data center industry's response to the COVID-19 pandemic and sets out recommendations, many of which will apply to future pandemics. These recommendations are based on established best practices; advice from expert bodies; roundtable discussions; and feedback and comments from Uptime Institute Network members and clients globally to the Uptime Institute Intelligence team and Uptime Institute consultants on five continents. See the Appendix for a list of relevant resources. Further reviews of the COVID-19 response and lessons learned will be published at (a) later date(s).

To further support owners and operators during the COVID-19 pandemic, Uptime Institute also provides regular bulletins with updates, recordings of live webinars, question and answer documents and other resources, found on our website, Uptime's Inside Track platform and LinkedIn.

Management: Strategic steps

This section provides strategic considerations for management. Further specific recommendations for managers, as well as tactical operational recommendations, are detailed in **Operations: Tactical steps**.

Plan a staged, multi-level response

The first and an essential step for management is to be prepared — develop a specific pandemic preparedness and response plan. If a pandemic-specific plan is not in place, use another emergency plan that may have been prepared for civic or similar emergencies. Share the pandemic plan with all employees, stakeholders, vendors/suppliers and key customers. Establish a system whereby elements of the plan are tested, updated and changes disseminated on a regular basis. Address gaps in the preparedness and recovery plan on an ongoing basis.

The pandemic plan should incorporate a tiered response, clearly identifying the actions to be taken at each level and the circumstances that would trigger implementation of the next level. Most organizations have a three to five-level contingency plan, ranging from "normal" (pre-pandemic) operations, to taking reasonable precautions, through

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

lights-out operation and, in worst cases, a complete site shutdown with transfer of critical applications and operations to backup sites. The plan should be practiced or role-played if possible.

At every level, the plan should clearly identify the trigger(s) to implement that level, the decision-makers authorized to direct escalation to that level, and the appropriate actions for operations (including policies for facility access, on-site activities, staffing and sanitization).

The following should be clearly specified at every level:

- IT assets that are critical.
- Maximum acceptable downtime, reduction in redundancy and/or recovery time for all equipment.
- Disruption/failure response procedures.
- Minimum acceptable staffing levels (by roles) and designation of critical staff and alternates.
- Staff protection (e.g., temperature checks, contact tracing, reporting of symptoms).
- Site access.
- Minimum acceptable levels of critical on-site activities, such as equipment maintenance.

A tiered-response plan should include plans to meet the challenges of operating with reduced staff, including situations in which staff may be unable to access the site or may need to leave the site on short notice. It should include a staffing threat matrix for various scenarios of employee absenteeism (e.g., under 25 percent, 25-50 percent, 50-75 percent, 75-99 percent, 100 percent). For each scenario, summarize the following:

- Business impact – critical work.
- Business impact – noncritical work.
- Impact on service level.
- Impact on group metrics.
- Data center operations response elements by response tier, such as:
  - Changes to shift schedules and minimum site staffing levels.
  - Work-from-home requirements and designations of roles.
  - Isolation and distancing policies.
  - Required personal protective equipment (PPE).

Determine the preparedness of the emergency response team — the identification of specific individuals/roles and potential alternatives is important. Where practical, include triggers/provisions for external alternatives (i.e., the use of third-party experts/specialist staff) to cover as a contingency. The creation of a RACI matrix (roles/tasks mapped against who is responsible, accountable, consulted, informed) for different levels of response may be useful.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Recognize that any change from normal processes (e.g., reduced staff numbers, limiting interaction between shift teams, covering critical facilities remotely) can increase the risk of human error or extend response times in case of emergency.

For detailed recommendations to help manage risk and for specific guidance on these and other measures, see **Operations: Tactical steps**.

The plan should make provisions for a multi-peak/wave pandemic, taking into account a second wave, possibly only weeks after the first and possibly worse, when supplies and finances are depleted, staff is fatigued, and maintenance has been deferred. Multiple waves/seasonal re-occurrences may also be likely. Long-term contingencies (e.g., vaccine not available, critical supplier goes out of business, etc.) should be considered and planned for as well.

Additionally, operators should plan for a staged step-down in pandemic-related measures as easing of conditions warrant. Just as the response moves up through escalating levels (i.e., increasingly rigorous responses to increasingly problematic circumstances), the path to ”normal” operations should follow a step-by-step de-escalation approach (i.e., owners/operators relaxing response measures gradually and with careful thought). Some measures (e.g., maintaining sanitation supplies, access controls, designation/training of alternates) may never be relaxed. (See also **Long-term planning**.)

Protect the business

Management should confer with insurance companies and legal advisors on relevant items, such as cleaning requirements, service level agreements (SLAs), notifications, etc. For data centers in areas where there is no clear regulatory mandate, management should decide — in consultation with insurance companies, legal advisors, Human Resources (HR) departments and other business unit(s) — at which response level to institute certain response measures (e.g., temperature checks, contact tracing, moving critical applications to alternate sites).

Some data centers are officially considered to be part of the critical national infrastructure. While this may confer some advantages, such as priority access to fuel, it may also mean that plans need to be shared with and agreed to by overseeing authorities.

As part of the strategic plan development, clarify the status of key data center workers (whether they are classed as essential workers) and of the data center (whether it is deemed part of the nation’s critical infrastructure). Determine precisely what these terms mean (it varies from country to country) and what documentation is needed for various situations (staff travel/shortage of fuel, etc.). (See also **Protect the site** and **Protect the staff**.)

Avoid unnecessary risks. Consider postponing or cancelling projects or activities that may increase the risk of infection, significantly increase the risk of an incident or failure, cause cash flow exposure (if this is a concern) or put strain on suppliers, partners and staff. As part

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

of postponing a project (or deferring maintenance) establish what conditions will need to exist before the project can be restarted, or maintenance tasks resumed.

Even with the best planning/communication, a pandemic will likely have impacts on data center operations budgets. Executive management will need to assess the situation and prepare accordingly. Government support is available in many countries.

Beyond that, as with the case with other abnormal events (e.g., equipment failure or severe weather event), management typically takes the reasonable approach of instructing operations team to spend what is necessary to protect staff and the data center infrastructure, keeping track of the costs.

Justifications of expenditures should be examined as a part of an ongoing review process. If management requires justification prior to expenditure, ensure that the case for all proposed spending is detailed, highlighting the risks to operations and staff if the expenditure is not authorized. The operations organization should be given clarity on which expenditures are deferred, which are approved, and levels of approval authority for any nonplanned expenses. (See also **Prepare for other disruptions**, **Develop a communications plan** and **Operations: Tactical steps**.)

Limit or closely manage travel

Travel limitations are applied by companies and governments during a pandemic. Government rules in affected countries should always be followed. Rules will be relaxed as a pandemic subsides; different policies should be applied at different times. We recommend the following:

- **Stop/reduce all unnecessary travel.** Organizations should be clear about what constitutes acceptable travel (for example, short local journeys versus longer/international travel) and develop appropriate guidance.
- **Prohibit or reduce travel between sites.** Where travel between sites is necessary, ensure cross-contamination is minimized — one site may be backing up another. (For detailed steps to reduce cross-contamination, see **Upgrade general sanitization** and **Manage staff shifts**.)
- **Secure documentation.** Staff and essential visitors may require documents or permits to travel to and from the site (see **Obtain documentation for exemptions**).

Prepare for other disruptions

Management should anticipate disruptions on multiple fronts.

External services

Understand the network paths of mission-critical IT applications and workloads. Review and revise backup/disaster recovery plans as necessary. The shift to more internet-based activities (e.g., e-commerce,

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

remote monitoring, telecommuting) means increased stress on bandwidth, the power grid, networking, etc.

Construction projects

A pandemic presents challenges for data center construction, major upgrades or extensions of capacity. Construction speed has a big impact on cost, and delays in one area can impact other areas and a range of suppliers. The impact of all potential disruptions, from the availability of staff to a shortage of construction material, must be assessed and weighed. Every project — indeed, every activity — in the data center should be examined to determine whether it can continue under the new conditions and response tier level. Tasks and projects that can continue without increased risk to staff or availability can proceed, while other tasks or projects may need to be delayed. As conditions change, reassess risks. If projects can or must continue, see **On-site construction projects** for recommendations.

Supply chains

Confer with suppliers to understand the risks — current and potential — for disruptions, including possible long-term disruptions, beginning with critical spares and consumables. Understand the geographic regions where key components are sourced and/or manufactured, and what the available alternatives are if supply chains are disrupted. (See also **Protect the site**.)

In addition to resources that are core to business functionality, we also recommend procuring and storing an appropriate supply level of products that reduce the spread of infectious agents (disinfectant wipes, hand sanitizer, masks, gloves, noncontact thermometers, the appropriate cleaning products for different types of equipment, etc.) Many of these products have expiry dates, so establish a procedure to keep supplies current and effective. (See also **Operations: Tactical steps**.)

Staffing

The graying of the workforce in some geographies means that despite best efforts, the data center industry may be more vulnerable than other industries to a pandemic. This presents a challenge, given the existing and well-documented staffing shortages the industry faces. A more age-diverse workforce may prove more resilient.

Be prepared to use alternative staffing vendors and to place these organizations on standby — if available and economically feasible. This may include using staffing resources (mobile workforce) and specialist staff (electrical/mechanical) from multiple suppliers. For tactical steps on managing operations staff, see **Manage staff shifts**.

Continuing education and training will be more important in the future; efforts to strengthen recruitment and training programs should be developed on an ongoing basis. Work with trusted partners to develop protocols for in-person and remote training. Focus on the content, which is more important than the delivery mechanism. (See also **Long-term planning**.)

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

The use of automation and remote monitoring can enable facilities to operate more effectively, and for longer, with less need for on-site staff. The pandemic will likely accelerate the long-term trend in this direction (the same applies to productivity and remote collaboration tools.) For details and recommendations, see **Use remote monitoring and management**.

It is important to note that unless there is adequate available staff, a pandemic is not an ideal time to implement a new remote monitoring or automation system on-premises (using a remote, cloud-based service may be slightly easier, but can still be challenging.) Implementing these systems is a staff-intensive project and requires dedicated technical and project (as well as ongoing program) management. However, it can be easier during a pandemic to secure a budget for future implementation, as the justification may be clear. As described above, this longer view planning process should include budgeting for these types of initiatives. (See also **Long-term planning**.)

Develop a communications plan

A pandemic is a dynamic situation. Stay current by consulting available information sources for updates and guidance (see **Appendix**). Use trusted, official, commercially independent sources.

Maintaining communication with employees, customers, suppliers and partners is critical. Frequent — daily or even twice-daily in the early stages — briefings may be appropriate as the conditions change and may affect business operations. Share news updates and links to public resources to keep staff informed of the current status of the pandemic and best practices for maintaining a safe and healthy work environment.

There are several specific considerations for communications, including the following:

- **IT service impacts.** Responses to a pandemic may affect internet traffic, workloads and availability requirements for some clients. Operators should confer with clients, internal and external, to discuss any impact, especially if upgrades or migrations are planned or new capacity is being added and if delays to those projects may impact business unit and/or client operations or projects.
- **Company policy and process.** Provide clear guidance to staff on company (and regulatory) policies related to symptoms (personally or in family members), cases of possible exposure, self-quarantine parameters and duration, and implications for sick leave/paid time off limits, insurance coverages, etc.

  Clarify the escalation process. Ensure that business units — especially mission-critical units — are fully briefed on response levels, the specific events that would trigger escalation and the potential impact of an increased response level on their business operations. Keep employees updated on a regular basis on the organization's current response level and its effect on daily activities. If activities such as operations and maintenance are outsourced, work with partners to set and align policies.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

- **Business/technical alignment.** Encourage business units (business functions and internal customers) to be in frequent communication about policy changes that may impact data center/IT operations. For example, directing employees to telecommute or instructing clients to use online services could drive a sharp increase in online traffic, for which IT should be prepared. (In the case of COVID-19, some retailers closed all of their physical retail stores and announced that their online store was still "open for business" — causing a surge in demand.)
- **Lessons learned.** Because many organizations have data centers in multiple regions, responses may vary by location or facility characteristics. Share lessons learned in the more affected regions with those less/not yet affected to strengthen their response. Ensure that there is no confusion between each region's response or level of response and global policies.

Operations: Tactical steps

While many of the steps that need to be taken involve external partners, protection of the immediate site and staff are the first concern. Although virus transmission is the subject of much research, little of that research is specific to data center environments. The recommendations below are based on findings from the World Health Organization (WHO), the US Centers for Disease Control and Prevention (CDC) and other major advisory organizations.

Protect the site

A necessary first step to protecting the staff is ensuring a safe work environment. The measures below help safeguard employees, clients and vendors and maintain business continuity.

Review procedures and policies

Ensure the completeness and accuracy of all procedural and policy documentation. Review disaster recovery plans, standard operation procedures (SOPs), methods of procedure (MOPs), emergency operation procedures (EOPs), statements of objectives, etc., and update as necessary for current and anticipated conditions. Role-play to confirm that all plans and procedures could be followed by a resource not normally working at the facility. Consider developing SOP and EOP orientation and training of vendors (remotely, to the extent possible) so they could perform basic functions in the event of a high level of absenteeism of the organization's regular staff.

Ensure that there is virtual (off-site) access to procedures (e.g., SOPs, MOPs, EOPs), policies and disaster recovery plans to allow for remote co-piloting if needed. Ready access to comprehensive procedures make it easier for two-person teams to work together when one person is

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

off-site, using video streaming services. In that way, a senior person can guide a less-trained person or an outside party through a step-by-step activity.

For some data centers, a pandemic may be an opportunity to update certain core materials. While projects and maintenance activities are reduced, staff can take advantage of the slower cycle to review and update plans and libraries (e.g., skill inventories, plans for upgrades, succession plans). This can be accomplished off-site. Similarly, this may be an opportunity to encourage documentation and knowledge transfer from experienced staff, in the form of annotating procedures and manuals, video conferences between relevant parties, etc. (See also **Long-term planning**.)

Examine (and re-examine) the resiliency of the facility's architecture — if redundancy is insufficient to accommodate failure of one or more components, develop alternative plans of action to ensure availability. Remember that some services previously considered noncritical may be relied upon more during times of pandemic. Also consider situations in which a reduction in redundancy (e.g., from N+2 to N+1) may have been considered acceptable in the past, but now presents a greater risk.

As always, have a plan in place to respond to any major problem, coordinating with vendors as necessary, to ensure issues can be addressed. Be prepared to deal with the possibility of a major equipment failure when key staff or resources may be unavailable owing to quarantine or supply-chain disruptions. Review EOPs to confirm that those procedures clearly address both what must be done to ensure the failed equipment is brought to a safe state when repair is not possible and what steps are required to provide continuity of operations (e.g., bypass, switch to redundant components, migrate load and/or critical applications to backup resources). Clearly communicate plans and procedures regarding equipment failures in these scenarios.

Control site access

Access to critical facilities, almost by definition, is strictly controlled already — this will prove helpful in reducing infection risks. Consider the following recommendations:

- Prohibit unscheduled visitors.
- Work in consultation with the organization's HR and/or Environmental Health and Safety department(s) to develop a screening questionnaire regarding exposure to high-risk situations (travel to high infection-rate locations, current symptoms or contact with others displaying symptoms, etc.). Require all individuals (employees and nonemployees) accessing the site to complete the questionnaire prior to admission.
- Send nonemployees the screening questionnaire via email 48 hours prior to their visit (or as far in advance as possible) and require completion before the appointment is confirmed. Verify that all answers remain unchanged upon arrival. Permit entry only if answers indicate a low probability of infection.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

- Because many healthcare providers are not able to test for the pathogen during a pandemic, adopt a conservative approach: Consider any related symptom as a possible case of infection.
- Security staff at the data center gates should inspect entry passes and any relevant health documentation. Entry to the site is allowed only if the visitor is qualified and cleared.
- Consult screening criteria guidelines issued by public health authorities. It may be appropriate to measure staff and visitors' temperatures by noncontact methods (if possible/available). Inform all who enter about the disease-mitigation efforts in effect (e.g., social distancing, use of PPE, hygiene and disinfection efforts). Post health self-assessment signs at all entrances and in high-traffic areas.
- Facilities operating in severely affected areas should monitor current conditions as they pertain to site security. Potential risk factors during a pandemic include:
  - Decreased availability of security staff.
  - Disabling of contact-based security technologies (see **Upgrade general sanitization**).
  - Civil unrest.

Analyze supply chains

Anticipate and prepare for supply-chain disruptions on items such as cabling, server racks, critical infrastructure spares and other components. Order more inventory for critical items and discuss projected lead times with vendors and suppliers. Where the site depends on vendors and/or service providers to maintain inventories of critical spares and consumables, verify that those vendors have anticipated and accounted for possible supply-chain disruptions. (See also **Prepare for other disruptions** and **Review procedures and policies**.)

Top off fuel tanks. Data center operators should ensure they have a priority delivery contract with fuel vendors. Operators without an existing agreement may not be able to negotiate one under pandemic conditions, but an attempt should be made. At the very least, discuss this eventuality with fuel suppliers: Ask what their plans are for delivery of fuel if shelter-in-place orders are given in the area. This will at least set a baseline in a worst-case scenario.

In extreme situations — for example, regions at high risk of shelter-in-place orders, areas susceptible to regular power outages, or situations in which the data center operator does not have a priority delivery contract in place — data center operators could consider having temporary fuel tanks or tanker trucks parked at the site. Remember that hospitals will usually get the first fuel deliveries in health emergencies.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Rank equipment maintenance

Infrastructure readiness must still be considered a high priority for mission-critical facilities. To ensure high availability is maintained, conduct a review of maintenance operations across multiple areas.

In accordance with industry best practice, categorize maintenance tasks as critical versus noncritical to facilitate prioritization. Deferred maintenance brings higher risk; in some equipment this risk is more serious than in others, so maintenance activities should be prioritized in order of criticality.

When prioritizing maintenance and testing activities, consider the following:

- The resources required to complete the activity.
- The risk of the activity both to site availability and to the health of staff performing the work.
- The risk of not doing the test or maintenance activity.
- The risk to the facility if the activity causes an event (i.e., extra resources may be required on-site to address the emergency, which may involve individuals who may not have been screened).

Contact the manufacturers of components/equipment to better identify the consequences of not performing or delaying maintenance on specific equipment.

Essential maintenance activities should be prioritized. If this is not possible, consider rotating operating hours as much as possible between redundant components. A short-term solution to the lack of maintenance /lack of vendor access is to train internal staff to perform small-scale maintenance tasks.

Postpone maintenance (e.g., infrared scanning and quarterly electrical power management system visits) and major projects where performing these tasks would increase risks to availability or staff health. If tasks do not pose increased risks, they can be performed as scheduled; reschedule high-risk testing (e.g., black start/plug-pull tests, generator load bank tests) for after pandemic risks have subsided.

As time passes and restrictions remain in place, revisit deferred tasks and determine whether continued delay increases risks beyond reasonable tolerances.

It is also important to plan for the restoration of “normal” maintenance activities. An influx of maintenance activities at once could pose additional risk, for example. To limit potential risk, consider a step-by-step approach to the resumption of deferred maintenance.

Note that while many data centers are busier during the pandemic, others (e.g., airlines) may be less busy than under normal conditions. Facilities in the latter category might consider performing maintenance activities, as long as adequate support in terms of staff and equipment is available and backup/recovery plans are up to date.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Upgrade general sanitization

In a pandemic, sanitization is, of course, crucial. Critical facilities present challenges, because of access/security, the need for specialized procedures and the need to protect equipment. The following steps will improve protection:

- **Intensify housekeeping measures.** Conduct multiple rounds of cleaning daily, especially of heavy-contact surfaces (e.g., door handles, light switches, elevator buttons, handrails, faucet handles). If possible, have a cleaner continually cycle through the facility disinfecting high-touch surfaces during hours of operation. (This includes workstations, offices and personal and shared technology.) Consider separate receptacles and processes for biohazards.
- **Remind staff.** Using signs and daily briefings, remind staff of their responsibility for sanitization. Post signs through the facility reminding staff to do the following:
    - Carry tissues and sneeze and cough into those tissues, then dispose of the tissues in a sanitary waste receptacle.
    - Wash hands thoroughly and often.
    - Disinfect all work areas at the beginning and end of each shift.
- **Provide supplies.** Ensure the availability of adequate PPE, including masks, gloves and biohazard suits, as well as cleaning materials, hand sanitizer, tissues, disinfectant wipes and appropriate waste receptacles. (See also **Supply chains**.)
- **Evaluate the level of cleaning appropriate for each setting.** Although it is common to use “clean,” “disinfect” and “sanitize” synonymously, the materials, methodology and timeframe of action can differ. Consult cleaning contractors and relevant public health/regulatory authorities to determine the most appropriate methodology and frequency for each situation.
    - *Cleaning* removes dust, dirt and other impurities from a surface by scrubbing/washing with a water-based solution of soap or detergent, then rinsing. This is a physical process that lowers the number of infectious agents on the surface. Deep cleaning in a data center setting involves cleaning around sensitive electronics, as well as in plenum spaces and beneath raised floors, using equipment with high efficiency particulate air filters.
    - *Disinfecting* inactivates the microorganisms identified on the product’s label (e.g., bacteria, viruses and/or fungi). This is a chemical process that does not necessarily remove any dirt or the infectious agents it inactivates from the surface. A disinfectant inactivates nearly 100% (99.9999%) of the relevant strains of microorganisms on a surface within 5-10 minutes.
    - *Sanitizing* reduces the number of microorganisms on a surface (the specific microorganisms the product can address are

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

identified on the product's label). This process may involve either cleaning or disinfecting. Sanitizers reduce the number of microorganisms on a surface to a level considered safe by public health standards (99.9%) within 30 seconds.

- **Evaluate entrance security technologies for transmission risk.** For example,
    - Consider alternatives to security technologies that require skin contact (e.g., fingerprint readers). If alternatives are not available, sanitize equipment before each use (not after — a passer-by could contaminate it between uses).
    - Person traps (physical security access controls that comprise a small space with two sets of interlocking doors) could present a repository for a virus — they are contained spaces, they are not usually well ventilated, and they have surfaces that could allow a virus to live for hours/ days. Consider limiting the use of person traps and/or sanitizing after each use.
- **Use spray disinfection or fogging techniques where possible.** These are more effective than simply wiping surfaces with disinfectant solutions, as the antiseptic mist coats surfaces for a longer period. Consult cleaning contractors and equipment vendors to determine acceptable sanitizing systems for specific areas of the data center.
- **Review the procedures and materials used by contracted cleaners.** Consider hiring a specialist cleaning firm that follows recommendations for sanitization from recognized public health authorities.

Shared environments

Consider closing all common areas. This may include fitness centers and cafeterias in facilities, keeping open only kiosks/micro-markets with prepackaged food.

Avoid workspace sharing. Most data centers have limited workspaces for staff (e.g., building management system [BMS] room, operations office). If possible, designate meeting rooms or other spaces for shift staff to use on an alternating basis — for example, the day shift uses the operations office, the evening shift uses the conference room, and night shift uses facility manager's office. Set up BMS consoles and network access so that shifts do not have to enter each other's workspaces. Where this is not possible, institute procedures to sanitize the shared spaces between shifts. (See also **Manage staff shifts**.)

Avoid equipment sharing. To the extent possible, avoid sharing equipment — provide each staff member their own resources. If equipment must be shared (e.g., shift phones, radios, tablets, tools, keyboards), sanitize at the start of each shift. (See also **Manage staff shifts**.)

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Consider specialized sanitization

White-space/IT environments

Research and adopt methods of deep cleaning a white space environment, considering the specifics of the facility (e.g., air exchange rate/volume, raised floors). Increase the frequency of standard cleaning operations (i.e., public spaces, equipment cabinet exteriors, etc.).

The need for deep cleaning (full wipe down/sanitization of all equipment, cleaning under raised floor and above suspended ceilings, disinfectant fogging, etc.) should be assessed. It can be extremely expensive ($1 per square foot), time-consuming and may even introduce risks; many areas subjected to a site-wide deep clean are very rarely accessed by staff or visitors. Even so, a deep clean may be advisable at the outset, or at certain time/intervals; viruses are more likely to remain active longer on dirtier/dustier surfaces.

Consult design/engineering consultants and/or equipment manufacturers as appropriate. Discuss the materials and procedures to determine potential impacts on specific equipment. There are many products designed to clean and disinfect electrical equipment (see **Appendix**).

Begin outreach to identify specialty cleaning vendors for technical space/equipment areas (white space, data halls). Apply the same diligence used in vetting any critical contractor — inquire about their experience with this type of deep cleaning, past and current clients, what methods are used, etc. Obtain specific information for the following scenarios:

- **Precautionary (suspected or no infection)**. Ensure that cleaning staff use specialty cleaners and cloths that are approved by the appropriate disease control authority in the region, and that all materials used in the cleaning are removed from the facility and disposed of as a biohazard once cleaning is complete.
- **Confirmed infection.** In addition to the steps above, ensure that cleaning staff use biohazard suits, gloves, shoe coverings, etc.

Air filters

Based on information available at the time of publication, the coronavirus that causes COVID-19 is more likely to be spread through proximity to infected individuals than dispersed via ventilation systems. It is currently believed that filters are unlikely to play a large role in mitigating the spread of COVID-19 in data centers, but research continues and guidance may change.

Review the scheduled replacement of make-up air intake filters and heating, ventilation and air conditioning unit air filters. Consult manufacturers, service vendors and industry advisory groups (e.g., ASHRAE, the National Air Filtration Association) for guidance on filter specifications, replacement and the safe disposal of used filters.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Fire systems

It is common during various housekeeping operations to put the fire system into bypass. This is especially important if there is a very early smoke detection apparatus system present, which can be triggered by disturbances of even very small particulate (they are specifically designed to be highly sensitive). Our recommendation is to put the fire system in bypass while cleaning (maintaining compliance with local jurisdictional requirements). This may require fire watch or similar measures be taken while the system is in bypass.

Other sanitization methods

Based on information available at the time of publication, it is thought that interventions such as negative pressure, ozone treatment and ultraviolet germicidal irradiation (UVGI) using short-wavelength ultraviolet C (UVC) light to kill or inactivate microorganisms have prohibitive downsides for either the equipment in data centers or the humans who staff them. However, research continues and guidance may change.

There has been specific interest in UVC light lamps and robots, which are commonly used to sanitize water, objects such as laboratory equipment, and spaces such as airplanes and buses. While UVC light in the wavelength typically used in UVGI applications can destroy viral genetic material, it can also cause irreparable damage to eyes, skin and, ultimately, the genetic material of people who are exposed to it. Additionally, UVC can disinfect only where it is directly applied — which makes it difficult to use in a data center where there are hidden areas, such as under raised floors, in overhead plenums, behind cabinets and cables, etc. A moving UVC robot (automated or remote controlled) has been proposed, but in critical spaces, this may create risks of collision damage or unintended activation of a critical distribution element (such as knocking against a switch, a valve or an emergency power off control).

While there have been studies regarding UVC in other settings, we are not aware of specific research relating to use in a data center and the possible impacts to cables, critical equipment and IT devices from long-term UV damage. One possibility that has been raised is the use of UVGI inside air ducts or plenums. This would likely have an impact similar to that of filtration (see **Air filters**).

Based on currently available information, the rigorous adherence to a program that includes hand hygiene, surface cleaning and physical distancing will reduce the likelihood of disease transmission without introducing additional risks — which is often the case with sanitization methods that are novel or not already widely used in data centers.

Use remote monitoring and management

A key goal during a pandemic is to limit site traffic.

Data centers should use remote monitoring, remote management and remote automation software/systems where possible, and especially when they are operating with smaller number of on-site staff and/or with

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

reduced staff shifts. If these capabilities are limited or not available, we recommend data center operators invest in these software/systems for the long term.

Organizations should also explore remote, cloud-based monitoring services (which are managed by the supplier). Although the capabilities of cloud-based services are typically limited compared with more complex, on-premises (installed on-site) software/systems, they can provide critical alerting and alarming (and their capabilities continue to be developed). However, even remote cloud-based monitoring services can still require that the appropriate sensors and meters are already installed.

In a worst-case scenario, remoting monitoring and automation software/systems and/or services can make it much easier to operate a facility remotely, with no staff on-site (although of use of automation requires careful thought and testing). It may be possible to defer critical repairs and replacements in such a situation.

The organization's policy toward remote data center management software/systems/services and security may need to be reviewed. Some organizations enable remote network operations centers, remote facilities monitoring and provide technicians remote access through private network connections. These organizations may be better prepared for pandemics. (See **Long-term planning**.)

Others do not allow remote monitoring or remote connections because of security concerns or other concerns around safety/availability or the need for expert on-site oversight.

Note that if staff must be evacuated or a data center is reduced to a skeletal staff, the ability to continue to operate will depend to a great extent on the facility design. A data center with enough infrastructure redundancy to meet Uptime Institute's Tier III or Tier IV standards is more likely to be able to continue to operate for a sustained period — especially with good monitoring.

Protect the staff

Working practices, legislation and attitudes to working conditions and/or safety can vary significantly from country to country. Similarly, rules regarding telecommuting, remote access to data, and on-site attendance can vary widely by country and industry. The following suggested practices should be considered in association with HR and/or IT security management.

Authorize remote working

Stress test all virtual private network (VPN) connections and validate broadband capacity to ensure reliable access during higher volume/frequency of virtual interaction, then consider instructing all staff noncritical to data center operations to work from home. Consider postponing/cancelling all in-person meetings (both internal and external) — use email, phone and audio/video conferencing.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Provide city/region-specific instruction on which VPN server to log into (particularly important since most of company's workforce will, at least temporarily, be telecommuting).

Ensure VPN access to the BMS and, if available, other remote monitoring, management and automation software/systems. As part of the overall operations continuity plan, consider requiring key on-site operational staff to work from a remote site at least once a month, if practicable. VPNs and all other software systems supporting critical equipment must, of course, be extremely secure, and it is wise to conduct a thorough security review using external experts.

Ongoing team communication is critical. Establish protocols by which teams isolated from each other communicate virtually (e.g., by radio, phone/video conference) with one another on a set schedule and test the communication platform/system in advance.

Obtain documentation for exemptions

Most "lockdowns" make exception for people going to work; however other authorities having jurisdiction (AHJ) may apply stricter controls on travel within their areas of control.

Contact local authorities to confirm exemption status, and lobby for this if it is not already explicit. (A more detailed discussion of data center staff/vendor exemption status for COVID-19 is provided in our **Bulletin No. 2, COVID-19 Update**.)

Management may need to obtain permissions/official documents that allow key employees to travel to work (especially if cross-border commutes are common in the area). Ensure site staff are prepared with documentation of their employment and, if appropriate, the organization's COVID-19 response plan.

Plan for essential maintenance visits. Some governments or companies may relax rules, or provide exemptions, for the maintenance of essential equipment. Plan for how to manage this in advance and obtain the necessary permissions where required. Permissions may depend on the applications/services being run in the data center. (See **Protect the business** for more on this this topic.)

Manage staff shifts

Ideally, the principles of redundancy that underpin data center design and operation should apply to the staff as well. In many sites, of course, such principles are already applied. During a pandemic, we recommend the following actions and considerations:

- Review designations of critical staff and alternates and confirm that alternates have been fully trained and briefed on the roles and duties of the critical employees they may need to temporarily replace.
- Create teams of mission-critical staff, ensuring each team has a mix of skills/experience sufficient to effectively manage the

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

facility (if this is appropriate and if the site is adequately staffed). Segregate teams between sites, especially by not allowing staff who work in a primary site to visit that site's backup location or have any contact with the backup site's staff. If possible, organize site tasks so that teams work in separate areas of the facility, never coming into contact with each other or the others' workspaces. (See also **Shared environments**.)

- Ensure that team members always work the same shift, so there is no cross-shift contact. Allow no cross-contact of teams, even outside the work environment. Incoming shift workers should maintain at least a 6-foot (roughly 2-meter) distance from the outgoing shift workers, including in elevators. Where feasible, make shift handoffs contactless; conduct turnover conversations via phone or video conference, and monitor items normally checked during shift rounds/walkthroughs remotely.
- Some operators may extend shifts to 10 or 12 hours — but weigh this against the additional risks of longer shifts in terms of worker fatigue/human error, as well the potential additional cost of overtime pay. We recommend the following:
  - Limit extended shift schedules (e.g., 12-hour shifts) to two or three consecutive days and provide sufficient days off to allow staff to rest and recover.
  - Ensure all extended shifts include long, regular breaks.
  - Manage overtime so that no individual works more than 10 percent overtime on a monthly basis in consecutive months, or more than 20 percent overtime in any one month.
  - Do not allow total hours worked per person to increase.
  - Arrange shift schedules so staff can rest adequately between shifts.

Operators adopting the two-shift, 12-hour strategy may consider sequestering the third shift, holding the staff in reserve in case anyone in the primary crew exhibits symptoms.

Shift leaders should report regularly (via email) to managers on staff compliance with mitigation efforts (cleaning, physical distancing, etc.) and notify of any concerns (e.g., worker issues, shortage of disinfecting supplies).

Consider implementing a contact tracing system. Register the health information and location of staff, supplier staff and other related staff every day to monitor for possible exposure to the virus or any symptoms.

Data centers in severely affected areas or affected by curve-flattening efforts may consider additional steps to secure the workforce, including:

- Designating at least one self-quarantined individual per position per shift to be on call for emergencies.
- Given that the incubation period for COVID-19 is believed to be two weeks, consider bi-weekly rotations for teams working shifts: Team A works for two weeks in a distinct area with no crossover with any other teams. Then the next two week period, Team B takes over

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

and Team A self-quarantines for 14 days. (Self-quarantine includes having minimum physical contact outside of immediate family and taking common-sense steps to minimize the risk of contracting the virus, including avoiding public places and public transport.)

Consider emergency housing

Provisions for housing staff on-site should be considered only as a last resort, as doing this may actually spread a virus more rapidly. Many other issues — around liability, rest, food and sanitation, etc. — would need to be addressed. Instead, if possible, identify a hotel close to the site (ideally within walking distance) that can be used for staff to rest between shifts. Ensure the environment (hotel or on-site living quarters) is conducive to good physical and mental health (a clean, private, quiet sleep space; access to a variety of fresh, healthy food; access to showers, recreation and exercise facilities, etc.).

Some disaster recovery plans include providing accommodation for several family members for up to 2 weeks to avoid traveling to and from the data center. Uptime Institute considers this an extreme strategy that should only be considered in very rare circumstances. While the data center is perceived as a controlled-access space, it is not a safe space. Therefore, any organization considering this option should also consider offering a specialized education program for family members that includes awareness of the hazards and associated risks, emergency evacuation procedures and other relevant training.

Limit on-site consultants and vendors

The most predictable and routine tasks, conducted by expert in-house or contracted staff very familiar with the environment, have the lowest risks. Operators should attempt to eliminate other factors, processes and behaviors that introduce uncertainties. The management of third parties needs active attention. (See **Management: Strategic steps** for more on this topic.)

Eliminate (to the extent possible) all vendor access that is not necessary, and actively screen those who must visit. Ensure they are fully informed of all requirements and procedures currently in place. Review vendor training program and add topics and information to cover enhanced health and safety procedures and site work rules.

In addition to other recommendations in this report (see, for example, **Protect the site**, **Track suspected or confirmed infection** and **Use personal protective equipment**), if a consultant or other necessary visitor is required to be on-site, consider the following precautions:

- Set aside a bathroom for the visitor’s exclusive use. Disinfect it when they depart.
- Set out clear rules for bring food and drink on-site, for consumption and hygiene practices.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Coordinate with third-party service providers

According to Uptime Institute research, two-thirds of all sites use some form of outsourced services, which may be problematic if these firms cannot meet the terms of their SLAs. Close coordination among all companies concerned is needed to ensure that staff are not confused by conflicting advice/policies. Liaise with partners on response policies/escalation procedures and establish how frequently and by what means all parties will keep others updated. (See **Management: Strategic steps** for more on this topic.)

Review the terms of all SLAs with regard to staffing levels per shift and other terms. Contact service providers to discuss their ability to meet all requirements.

Check whether service providers might be able to offset local staff shortages by transferring experienced workers from another region. Consider that some people traveling to a new site may face quarantine periods, regardless of whether they have any symptoms. This quarantine would greatly reduce the availability of vendor staff in some specialties. Discuss these possibilities in advance. Determine if local service providers and vendors have plans in place to bring in (or secure remote support) factory technician resources for maintenance situations that exceed the skill and knowledge levels of locally based technicians.

Track suspected or confirmed infection

In addition to other recommendations (see, for example, **Consider specialized sanitization**), people who have symptoms; who have tested positive; who are caring for someone who has symptoms or has tested positive; or who have reason to believe they have been exposed to infection, including close contact with a confirmed case of infection, should be instructed to do the following:

- Follow all corporate and government guidelines related to reporting and self-isolation.
- Telecommute for the appropriate quarantine period (usually 14 days for COVID-19).

Consider “recovered” COVID-19 staff both potentially infectious and at risk until there is a clear guidance from health authorities on this issue. There are reports indicating that people who have contracted the virus and recovered have only limited immunity and may become re-infected. Therefore, all the same rules and policies should apply to all staff: Until more data becomes available, consider staff who have had COVID-19 to be both as potentially infectious and as at risk as all other staff.

Use personal protective equipment

Use of PPE is critical to helping mitigate the spread of infection, particularly when a person infected by a pathogen may be asymptomatic. However, staff and management should not focus so much on PPE related to disease prevention that they forget other, more routine safety

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

measures and PPE. That is, in addition to masks and gloves, staff working at heights should employ safety harnesses; staff working with electrical gear should wear correct dielectric gloves and PPE that corresponds to the level of shock hazard; staff working in closed spaces, such as fuel tanks, should use respirators; and so forth.

Also consider that wearing a mask and/or gloves can create a false sense of security: remind staff not to neglect other infection avoidance precautions, such as physical distancing and hand washing.

Face masks

Governmental and health authority recommendations (and in some areas regulations) on wearing face masks in public and/or in places of work vary widely. Taking this into consideration, if local government or AHJs in the area mandate use of masks, those mandates should be followed.

In localities where there is no mandate from government or AHJ, at minimum follow the recommendations of local health authorities.

If mask use is mandated or recommended, or if it becomes company policy to require masks be used as an additional precaution, management should formulate and communicate a policy on mask use, disposal, etc. with the intent of removing any potential points of contamination. The following are general guidelines and procedures for using masks that should be included in the policy:

- People who have symptoms, who have tested positive, who are caring for someone who has symptoms or has tested positive, or who have reason to believe they have been exposed to COVID-19, should self-quarantine.
- If a critical employee who may have been exposed to COVID-19 but is not showing symptoms must come into the data center, they should follow the guidance of the appropriate disease control authority, such as the CDC, on using a mask to limit the chances that they will spread the disease.
- Using masks does not reduce the need for physical distancing, frequent and thorough hand washing, and good sanitization.
- Follow instructions for proper use of masks, including putting the mask on, taking it off, and properly disposing of used masks, such as the advice provided by the WHO.

Note that if forced to reuse a mask, or if a mask is not disposed of properly, there is an increased risk of contamination. N95 masks use electrostatic filtering, which will likely be rendered ineffective by cleaning.

For data center operations, key times to use masks would include shift turnover, when staff are in contact with or escorting vendors or visitors, and when a key staff pair (e.g., senior employee and trainee) must be in proximity. In rare circumstances where a designated “critical” employee and that employee’s designated alternate must be in the same room, both should wear masks and maintain 6-feet (2-meter) physical distancing. (For more on this, see **Manage staff shifts**.)

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Work in arc flash environments

First, avoid doing any such work if possible.

In most instances, staff work within the arc flash protection boundary for a limited time, while isolating equipment so that work can be conducted in a de-energized state. Use an arc flash-rated full face visor to cover the entire face. NFPA 70E (a standard issued by the US-based National Fire Protection Association, a widely accepted source of good guidance on safe electrical work practices) does not allow any conductive, flammable or meltable materials on the face when working inside the arc flash protection boundary. Therefore, workers should employ other pandemic-related safety measures — for example, extending the limited approach boundary to 6 feet (roughly 2 meters) — to help prevent the spread of the virus for the limited time work is being conducted on live energized devices inside the arc flash protection boundary. All unprotected and unqualified people should be outside the extended limited approach boundary. Once the equipment is de-energized, the worker can remove the visor and, if policy requires, use a face mask.

Gloves

Use only single-use, disposable gloves that are discarded in an appropriate waste receptacle immediately after use. Follow approved procedures for glove use and disposal, taking precautions to avoid cross-contamination.

Work gloves and electrical personal protective equipment gloves are not suitable for sanitization procedures.

Encourage emotional well-being

Anticipate and make provisions for staff mental health/emotional well-being. This includes promoting self-care activities, such as eating well-balanced meals, getting sufficient rest and exercise, pursuing hobbies and maintaining healthy relationships. Consider encouraging staff to explore appropriate web-based resources, such as:

- Articles with tips and strategies:
  - **Space stress: How astronauts manage their mental health**.
  - **Focus on your behaviors to relieve coronavirus anxiety**.
- Crowd-sourced resource libraries and interactive groups (see, for example, the **Coronavirus Tech Handbook**).
- Online events/remote access entertainment offered by sports teams, zoos, musicians, etc.

Consider implementing a “buddy” scheme, in which colleagues engage in daily or least frequent communication with others.

Remind staff of support available through their benefits packages (e.g., confidential counseling).

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

On-site construction projects

For those organizations involved in data center construction, major upgrades or extensions of capacity, a pandemic presents both strategic and tactical challenges. (For more on the former, see **Protect the business**.) The cost of a project can be heavily impacted by the speed of construction. Delays can have a ripple effect, including across different areas of the project and affecting other suppliers. In this case, however, delays may be advisable, and the following actions may be appropriate.

Suspend all nonessential construction projects when possible. Evaluate the risks (availability and health) inherent in each project and determine appropriate actions. Where projects are allowed to continue, communicate and strictly enforce the revised work rules. Coordinate with contractors to ensure all subcontractors/vendors are applying appropriate safeguards.

If possible, create a separate, secure entrance for all parties involved in the project. Limit contact between project staff and operations staff to the maximum extent possible without compromising operational oversite of project work. Ideally, operations team members who are assigned to project oversight or supervision should be dedicated to solely those duties.

Projects may encounter delays that, depending on the language of the contract and how each country/jurisdiction interprets force majeure clauses, may carry financial implications. Owner/operators should document every delay in detail. Contractors should work with the insurer and the owner/operator to keep them informed of any problems so all are aware of the situation and can plan and prepare for the inevitable negotiations for the allocation of costs.

Where practicable, follow other recommendations in this report — see, for example, **Control site access** and **Protect the staff**.

Colocation and mixed-use facilities

In addition to the other considerations discussed in this report, colocation/multi-tenant data centers and mixed-use facilities face strategic and tactical challenges that single-occupant or dedicated facilities may not. See **Management: Strategic steps** for management-focused guidance; additional operational/tactical measures are discussed below.

Colocation/multi-tenant data centers

Colocation/multi-tenant data centers are likely to have more visitors than private enterprise/single-occupant data centers. There are usually more customers on-site, more potential customers, and a wider variety of maintenance staff. In addition, each may have different policies, SLAs and access rights. For these reasons, close liaison is essential.

There are likely to be situations where SLA breaches occur — for example, on levels of redundancy or on-site staff. Financial penalties and problems with customers may be avoided if all parties consult in

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

advance. (In addition, future contracts should be drawn up that clarify the procedures to be followed in the event of another epidemic — see **Long-term planning**.)

To avoid inconvenience and potential client dissatisfaction, be proactive: Notify all affected parties of the pandemic preparedness plan in place and its impact on their access to the facility in advance. These communications should stress that the steps being implemented are intended to support maximum availability of the data center infrastructure to the benefit of the clients.

Inform customers of the technologies available that allow them to manage workloads remotely (e.g., remote monitoring via data center infrastructure management dashboards, smart hands, etc.). Consider offering free or discounted rates on remote technologies to encourage use.

Suggest clients test their ability to respond to events remotely or using only on-call personnel before it might become necessary.

Postpone other nonessential on-site events (e.g., ribbon cuttings). Conduct virtual tours only.

In addition to the other recommendations detailed in this document (see, for example, **Control site access**, **Upgrade general sanitization** and **Protect the staff**), the following advice should be considered:

- Install glass shields at reception desks. Where possible, receive customers at a separate entrance on the periphery of the campus and, maintaining at least 6-feet/2-meter distance between all parties, escort customers to their assets.
- To support physical distancing efforts, use traffic-control methods (e.g., outlined walkways, barriers).
- Post signs at all building entrances, person traps and high-traffic areas about sanitization and protective practices.
- Limit the accessibility to shared spaces, such as client lounges, etc. Ensure there are sanitization supplies (and waste disposal units) in all shared areas, including next to vending machines.
- Consider closing all customer access for package pickup, by cleaning and delivering the shipments to customer cages or transitional space within the facility.
- In complexes, assign operations and technical staff members to a single building, and designate an entrance for their exclusive use (i.e., not used by other staff or customers). Prohibit cross-building access.

Mixed-use facilities

Some small data centers, sometimes designated as server rooms, are sited in mixed-use buildings, such as headquarters, factories or administrative centers. In this situation, while the principles described in this document largely apply, policies and rules will likely be set by noncritical facilities management.

Requirements (maintenance, site access, etc.) for critical staff, and for critical facility exceptions to the general building rules, should be clearly identified to establish exception policies where appropriate.

Long-term planning

In the past 20 years, viral outbreaks such as SARS (severe acute respiratory syndrome), MERS (Middle East respiratory syndrome) and COVID-19 have already caused death and economic disruption. Globalization means there will be more, and some could be much more deadly than those to date. Therefore, all organizations need to be prepared at all times, just as they are for more mundane and local disruptions, such as power failures. This means all actions should be planned and reviewed as a matter of routine good practice. This risk should also should inform investments in staffing, redundancy and remote management/automation.

The current thinking is that the COVID-19 virus may become endemic — recurring on an annual basis, much like the flu, or moving through certain geographies in waves. While dealing with the immediate challenge of the current global health crisis, business must also plan for the longer term.

Business continuity plans should be updated to include forward looking, preventative health measures (e.g., requiring essential staff to be vaccinated at the start of each flu season) and facility preparedness measures (reviewing digital resilience, site redundancy, vendor SLAs, etc.) as discussed in this advisory report.

Future SLAs and business contracts should clarify the procedures to be followed in the event of another epidemic, to help avoid financial penalties and problems.

Following COVID-19, some businesses will remain in a reactive mode until the danger has clearly passed; eventually this will be replaced by review and iterative improvement of policies and procedures. Many others, particularly with mission-critical IT, will very likely place an increased emphasis on contingency planning — not just for the next pandemic but for the next major, “unforeseen” event.

More detailed and more frequently reviewed and updated business continuity plans and disaster recovery plans are likely. We expect there will be more formalization (and where possible, simplification) of procedures to allow less qualified staff to perform those procedures.

Contingency plans and procedures will also place greater consideration of the availability of spare parts and supplies lists and levels. Many will evaluate primary and alternative vendors and vendor SLAs. There may be greater use of dual sourcing, which in recent years has become less common for economic reasons.

In regions severely affected by the pandemic, it is likely that many of the plans, policies and practices created to respond to COVID-19 will become

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

permanently incorporated into critical facility management. This may increase overall costs. However, none of the practices adopted during a pandemic should be maintained in perpetuity without appropriate evaluation of the costs and benefits. For example, home working saves commuting time and office overhead costs, but those savings must be offset against the benefits of in-person contact with co-workers and the availability of staff on-site in case of unforeseen events.

Other likely outcomes, which we are already seeing, include an increased emphasis on the availability of skilled staff with appropriate qualifications. There is a perceived need to "deepen the bench" to accommodate staff illnesses and absences. This should encourage greater and more focused staff training, particularly for critical employees and their alternates to ensure surrogates are fully prepared to step in if needed.

Although many were well prepared for COVID-19, more organizations will likely formally document which staff are essential to keep on-site during an epidemic, and which staff (and/or third-party suppliers) will provide backup. Pre-COVID-19, many operations teams already knew who those people were, but this was rarely documented. Uptime Institute will produce an advisory report for developing permanent processes/strategies as the lessons from this pandemic are learned.

Appendix: Resources

Global

World Health Organization Coronavirus disease (COVID-19) Pandemic

> With offices in countries worldwide, the WHO is leading the global effort to support countries in preventing, detecting and responding to the pandemic and monitoring the response. The WHO offers online COVID-19 training on a range of topics in multiple languages via the OpenWHO platform.

Asia-Pacific

The State Council – The People's Republic of China New Coronary Pneumonia Outbreak Prevention and Control Service Zone

> COVID-19 prevention measures, guidance, safety practice and information from each province in China.

Europe

European Centre for Disease Prevention and Control (ECDC)

> Risk assessments, public health guidance and advice on response activities related to the COVID-19 pandemic in European Union (EU) Member States and the EU Commission.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

European Commission Coronavirus Global Response

Landing page for the European Commission's coordinated European response to the coronavirus outbreak in the areas of public health, travel, jobs/the economy, research, digital technologies and more.

North America

Government of Canada Coronavirus disease (COVID-19)

Information on health, financial, travel and other resources, including a range of downloadable infographics for businesses and public spaces (e.g., on physical distancing, hand washing, how to use/remove PPE).

Johns Hopkins University of Medicine Coronavirus Resource Center

Research findings, guidance and daily updates from global public health experts in infectious disease and emergency preparedness.

US Centers for Disease Control and Prevention

Information and updates on symptoms, infection rates and safety measures for different settings in multiple languages including American Sign Language.

US Occupational Health and Safety Administration

General and industry-specific infection control strategies for protecting workers from exposure to the coronavirus that causes COVID-19.

Uptime Institute COVID-19 resources

A collection of reports, webinars and related content on maintaining mission-critical data center operations and business continuity during the COVID-19 pandemic.

ACKNOWLEDGEMENTS

The Uptime Institute Intelligence team thanks Chris Brown, Fred Dickerman, Scott Killian, Scott Good, Juan Orozco, Ryan Orr, Matt Stansberry, Alex Tay, Richard Van Loo, Amber Villegas-Williamson, and global members of the Uptime Institute Network and Uptime's Inside Track community for their contributions to this report.

ABOUT UPTIME INSTITUTE INTELLIGENCE

Uptime Institute Intelligence is an independent unit of Uptime Institute dedicated to identifying, analyzing and explaining the trends, technologies, operational practices and changing business models of the mission-critical infrastructure industry. For more about Uptime Institute Intelligence, visit uptimeinstitute.com/ui-intelligence.

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED

ABOUT UPTIME INSTITUTE

Uptime Institute is an advisory organization focused on improving the performance, efficiency and reliability of business critical infrastructure through innovation, collaboration and independent certifications. Uptime Institute serves all stakeholders responsible for IT service availability through industry leading standards, education, peer-to-peer networking, consulting and award programs delivered to enterprise organizations and third-party operators, manufacturers and providers. Uptime Institute is recognized globally for the creation and administration of the Tier Standards and Certifications for Data Center Design, Construction and Operations, along with its Management & Operations (M&O) Stamp of Approval, FORCSS® methodology and Efficient IT Stamp of Approval.

Uptime Institute – The Global Data Center Authority®, a division of The 451 Group, has office locations in the US, Mexico, Costa Rica, Brazil, UK, Spain, UAE, Russia, Taiwan, Singapore and Malaysia. Visit uptimeinstitute.com for more information.

All general queries:
Uptime Institute
5470 Shilshole Avenue NW, Suite 500
Seattle, WA 98107 USA
+1 206 783 0510
info@uptimeinstitute.com

© COPYRIGHT 2020 UPTIME INSTITUTE. ALL RIGHTS RESERVED