COVID-19: MINIMIZING IT & DATA CENTER RISK

BGD E-GOV CIRT

COVID-19: MINIMIZING IT & DATA CENTER RISK

Prepared by: Risk Assessment Unit
BGD e-GOV CIRT

Date: March 2020

Sharing Indicator: TLP WHITE

1. Sharing Indicator

Traffic Light Protocol (TLP) The Traffic Light Protocol (TLP) was created to encourage greater sharing of sensitive information. It is designed to improve the flow of information between individuals, organizations or communities in a controlled and trusted way.

TLP	Distribution principle	Mapping with the business category	Description
RED	(1-to-1, strictly limited)	Confidential information	Sensitive information disclosure of which can harm BGD e-GOV CIRT or its external parties' reputation, operations, or includes personal BGD e-GOV CIRT team members or external parties' data and information which is treated as confidential information in BGD e-GOV CIRT agreements
AMBER	(1-to-group, limited)	Internal information	Incidents information and all other information which is not treated as a public or confidential
GREEN	(1-to-many, limited)(information security community or special interest groups)	Public information	Information which was disclosed publically in accordance with internal BGD e-GOV CIRT procedures or related agreements with external parties
WHITE	(1-to-many, unlimited)(no restrictions, public)		

Information classification according TLP in BGD e-GOV CIRT

2. Table of Contents

3. Document information

Document version No.: 2020 V 1.0			
Project Director	Tarique M Barkatullah	**Team Leader**	Tawhidur Rahman
Document status	Final	**Document version date**	22-Mar-2020
Prepared by	Md. Sabbir Hossain	**Preparation date**	22-Mar-2020
Reviewed by	Tamim Ahmed	**Review date**	

4. Executive Summary

This advisory report has been produced by BGD e-GOV CIRTs' IT Policy & Risk Assessment team with the goal 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 epidemics. This report is based on Uptime Institute Advisory Report.

5. Introduction

Coronavirus disease 2019 (COVID-19) is an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). The disease was first identified in 2019 in Wuhan, Central China, and has since spread globally, resulting in the 2019–20 coronavirus pandemic. Till preparation of this document (22 March 2020), total deaths due to this virus is tolled to 266073 & Total infection Number is 11184 around the world. In Bangladesh 27 Infected and 02 death recorded till date by COVID-19.

COVID-19 is a pandemic. In situations such as this, mission critical facilities face particular challenges, due to both the risk of unavailability of key staff through illness or quarantine and other long term impacts that might affect the ability of the operator to maintain continuous availability. Fortunately, preparedness is in the industry's DNA; 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 the current pandemic.

As the virus spreads, more organizations are moving from updating their response plans to implementing them. Each organization is different, and responses vary based on site environment, the number of COVID-19 cases in the area and government-mandated restrictions. One thing all companies hold in common, though, is their priorities:

- The health and safety of their staff, partners and customers;
- Business continuity; and
- Compliance with the guidelines and regulations issued by public health and government agencies.

This report reviews the status of the data center industry's response to the pandemic and details recommendations and possible next steps.

6. Prepare the Business

A first and essential step is to be prepared. This includes the following components:

- Develop a specific pandemic preparedness plan. If a pandemic specific plan is not in place, use another emergency plan that may have been prepared for civic emergences, etc. The 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 taking reasonable precautions through lights-out operation and, in worst cases, a complete site shutdown with transfer of critical applications and operations to backup sites. The plan should consider situations in which staff may be unable to access or leave the site on short notice.
- Confer with insurance companies and legal advisors on relevant items, such as cleaning requirements, service level agreements (SLAs), notifications, etc.
- Consider IT service (client) impact. Responses to COVID-19 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 delays to those projects may impact business unit operations or projects.
- Maintain communication with staff, customers and partners. This is a dynamic situation, so frequent — daily or even twice-daily 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 (see Appendix).
- Provide clear guidance to staff on company policies (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.
- Keep employees updated on a regular basis of current response level and its effect on daily activities.
- If activities such as operations and maintenance are outsourced, collaborate with partners to set and align policies.
- Anticipate supply chain disruptions. In addition to resources core to business functionality, procure 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. Also, consider potential long-term disruption to the supply chain for critical spares and

consumables. Components made in China or other areas impacted may not be readily available for months. (Note that several major manufacturing plants for heating, ventilation and air conditioning [HVAC] equipment are located in Italy.)

- Avoid unnecessary risks. Consider postponing or cancelling projects or activities that may increase the risk of infection, cause cash flow exposure (if this is a concern) or put strain on suppliers/ partners/staff (see Consider factors that raise risk).

7. Protect Site

While many of the steps that need to be taken involve external partners, protection of the immediate site are the first concern.

Increase sanitization

- For a virus pandemic, sanitization is, of course, critical. 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 excludes workstations, offices and personal and shared technology.)
- Place hand sanitizer and disinfectant wipes (with disposal units) throughout the facility, as well as signs to remind staff and visitors to use them frequently.
- Place signs in bathrooms reminding staff to wash hands often, using proper techniques.
- Post signs through the facility reminding staff to carry tissues and sneeze and cough into those tissues, then dispose of the tissues in a waste receptacle.
- Note that person traps could present a repository for the virus in that they are small contained spaces, they are not usually ventilated, and they have surfaces that could allow the virus to live for hours, if not days. Consider limiting the use of person traps and/ or sanitizing after each use.
- Provide cleaning supplies and require staff to disinfect all work areas at the beginning and end of each shift.
- Review the procedures and materials used by the facility's contracted cleaning company. Consider hiring a specialist cleaning firm that follows recommendations for disinfection from recognized public health authorities (e.g., IEDCR).
- 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 your cleaning contractor and equipment vendors to determine acceptable sanitizing systems for specific areas of the data center.

- Research and adopt methods of deep cleaning a white space environment, considering the specifics of your facility (e.g., air exchange rate/volume, raised floors). Increase the frequency of both the standard cleaning operations (i.e., public spaces, equipment cabinet exteriors, etc.) and deep cleaning (full wipe down of all equipment, cleaning under raised floor and above suspended ceilings, disinfectant fogging, etc.). Consult specialist-cleaning firms, design/engineering consultants and/or equipment manufacturers as appropriate.
- Begin outreach to identify specialty cleaning vendors for technical space/equipment areas (white space, data halls) for two scenarios:
- Precautionary: cleaning personnel uses specialty CDC-approved cleaners and cloths. All materials used in the cleaning are removed from the facility and disposed of as a biohazard once cleaning is complete.
- Confirmed COVID-19 case at the site: cleaning personnel uses biohazard suits, gloves, shoe coverings, etc. All are bagged and removed from the site once cleaning is complete.
- Review the scheduled replacement of make-up air intake filters and HVAC unit air filters. Consider replacing filters more frequently and/or using filters with higher minimum efficiency reporting value rating.
- Ensure the availability of personal protective equipment, including masks, gloves and Tyvek (hazardous materials or hazmat) suits.
- Consider closing all fitness centers and cafeterias in facilities, keeping open only kiosks/micro-markets with prepackaged food.

Limit access

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

- Security checkpoints at the data center entry gates should inspect entry passes, take temperature measurement by noncontact methods (if possible/available) and disinfect (use sanitizers). Entry to the site is allowed only if visitor is qualified.
- Post health self-assessment signs at all entrances and high-traffic areas.
- Because many healthcare providers are not able to test for COVID-19 presently, adopt a conservative approach: Consider any related symptom as a possible case of COVID-19 infection. Consult screening criteria guidelines issued by public health authorities.
- Work in consultation with your organization's Human Resources (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 non-employees) accessing the site to complete the questionnaire prior to admission.

8. Protect Staff

Working practices, legislation and attitudes to working conditions and/ or safety can vary significantly from country to country. Similarly, rules regarding remote working, 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 security management:

- Test all virtual private network (VPN) connections to ensure reliable access, then consider instructing all staff noncritical to data center operations to work from home.
- Ensure VPN access to building management systems (BMS) for remote data center monitoring.
- Provide city/region-specific instruction on which VPN server to log into (particularly important since most of company's workforce will temporarily be telecommuting).
- Ensure access to standard operation procedures (SOPs) and emergency operation procedures (EOPs) to allow for remote copiloting if needed.
- Ensure SOPs/EOPs are accurate and could be followed by a resource not normally working at the facility.
- Depending on circumstances, consider postponing/cancelling all in-person meetings — use email, phone and audio/video conferencing.
- Remind staff (using signs, daily briefings) of their responsibility for sanitization — provide protection equipment, cleaning materials and reminders to wash hands thoroughly and often.
- Anticipate the challenges of operating with reduced staff.
- Developed 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).
    - Data center operations response elements.
    - Impact on service level.
    - Impact on group metrics.
- Research and test technologies for remote monitoring/ management (e.g., remote/smart hands), automation, etc. Stress test technologies and procedures in advance.
- Any staff member displaying symptoms should be instructed to self-isolate and telecommute for the next 14 days.
- Any staff who have had close contact with a confirmed COVID-19 case should be advised to self-quarantine for the appropriate period, usually 14 days.

- 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.

Limit travel

Travel limitations are being applied by companies and governments during the COVID-19 outbreak. Government rules in affected countries should always be followed. Rules will be relaxed as the pandemic subsides, so different policies should be applied at different times. The following should be considered:

- Ban/reduce all unnecessary travel. Organizations should be clear about what constitutes 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, take steps to ensure cross-contamination is minimized — one site may be backing up another.
- Plan for essential maintenance visits. Governments or companies may relax rules, or provide exemptions, for the maintenance of essential equipment. Most of the "lockdowns" currently in place make exception for people going to work, however other authorities having jurisdiction may apply stricter controls on travel within their areas of control. Operators must 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.

Manage shifts

Ideally, the principles of redundancy that underpin data center design and operation should apply to the staff too. In many sites, of course, such principles are already applied. During the virus outbreak, the following should be considered:

- Create teams of mission-critical staff, ensuring each team has a mix of skills/experience sufficient to effectively manage the facility (if this is appropriate and if the site is adequately staffed).
- Segregate teams between sites, especially by not allowing personnel 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. 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.
- Allow no cross-shift interaction. Incoming shift workers should maintain at least a 6-foot (roughly 2-meter) distance from the outgoing shift workers. This includes elevators.
- Shared workspaces should be wiped down with disinfectant wipes by the incoming shift staff.
- Depending on the appropriate medical or management advice, workers should use masks during shift turnover.
- Depending on the appropriate medical or management advice, training pairs (e.g., senior engineer and trainee) must wear masks at all times.
- Shift leaders should report regularly (via email) to managers on staff compliance with mitigation efforts (cleaning, social distancing, etc.) and notify of any concerns (e.g., worker issues, shortage of disinfecting supplies, etc.).
- Consider implementing a contact tracing system. Register the health information and location of personnel, supplier personnel and other related personnel every day to monitor for possible exposure to the virus or any symptoms (including those of the common cold).

9. Safeguard operations

To ensure high availability is maintained, review operations in these areas:

- In accordance with industry best practice, categorize tasks as critical versus noncritical to facilitate prioritization.
- Postpone all nonessential maintenance (e.g., infrared scanning and quarterly electrical power management system visits) and major projects where possible.
- If nonessential, reschedule high-risk testing (e.g., black start/plugpull tests, generator load bank tests) for after pandemic risks have
- subsided.
- Review disaster recovery plans, procedures and policies (e.g., SOPs, method of procedures, EOPs), statements of objectives, etc. and update as necessary for current and anticipated conditions.
- Develop SOP/EOP orientation and training of vendors (remotely, to the extent possible) so they could perform basic functions in the event of 100 percent absenteeism.
- Anticipate and prepare for supply-chain disruptions on items such as cabling, server racks, critical infrastructure spares and other components. Order more inventory 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.
- Develop plans to deal with the possibility of a major equipment failure when you may not have access to key personnel or resources owing to supply-chain disruptions.
- Ensure established procedures regarding equipment failures are clearly communicated. 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).
- Examine the resiliency of your architecture — if redundancy is insufficient to accommodate failure of one or more components, consider alternative plans of action to ensure availability.
- Top off fuel tanks.
- Stress-test VPNs to ensure systems can handle higher volume/frequency of virtual interaction, as many staff members will be telecommuting.
- Place alternative staffing vendors on standby (if available and economically feasible). This may include staffing resources (mobile workforce) and specialist staff (electrical/mechanical) from other suppliers.

10. Consider risk factors

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. In these cases, consider the following:

On-site consultants and vendors

- Eliminate (to an 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.
- If a consultant or other necessary visitor is on-site, consider instituting the following precautions:
- Set aside a bathroom for the visitor's exclusive use. Deep clean it when they depart.
- For visitors, vendors and consultants extend the general white space work rule of "no food or drink" to the entire data center property (i.e., non-staff are not allowed to bring food into the facility or use the employee break room).

Third-party facility management and other outsourced services

According to Uptime Institute research, two-thirds of all sites use some form of outsourced services. Close coordination among all companies concerned is needed to ensure that staff are not confused by conflicting advice/policies. Consider the following:

- Liaise with partners on response policies/escalation procedures.
- Establish how frequently and by what means all parties will keep others updated.
- 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.
- Discuss this possibility in advance.

11. Extra Cautions

In addition, in these areas, it is wise to adopt the strictest policies practical.

Enhance access restrictions:

- Consider prescreening all scheduled visitors before they arrive on-site.
- Send the visitor the questionnaire via email 48 hours prior to their visit (or as long 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.
- Prohibit unscheduled visitors.
- Institute temperature checks (using noncontact thermometers) before entry to the facility.

Further, secure the workforce:

- Consider designating at least one self-quarantined individual per position per shift to be on call for emergencies.
- Given that the incubation period for the virus 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 and Team A self-quarantines for 14 days. (Self-quarantine should involve minimum social contact outside immediate family and common sense health steps to minimize risk of contracting the virus, including avoiding public places and public transport.)
- Re-evaluate how food breaks are handled for site staff. Consider having a cleaner exclusively tasked with maintaining break room hygiene. Consider closing cafeterias and kitchen areas.
- Prepare for staff housing on-site, but use only as a last resort, as doing this may actually spread the virus more rapidly.

Further cleaning:

• Consult specialists to conduct deep cleaning on a regular basis throughout the facility.

On-site construction projects:

For those organizations involved in data center construction, major upgrades or extensions of capacity, the pandemic presents challenges. Construction speed has a big impact on cost, and delays in one area can impact many other areas and other suppliers. In this case, however, delays may be advisable, and the following actions may be appropriate:

- Suspend all nonessential projects when possible.
- If the project must continue, 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 and establish isolation of the project personnel from the operations personnel. Operations team members who are assigned to project oversight or supervision should be dedicated to those duties and not allowed to interact with the duty operations personnel.

Colocation/Multi-tenant data centers

Colocation/multi-tenant data centers are likely to have more visitors than private enterprise data centers. There are usually more customers visiting, 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. (In addition, future contracts should be drawn up that clarify the procedures to be followed in the event of another virus epidemic.) Actions to take include:

- Postpone all tours or other nonessential on-site events (e.g., ribbon cuttings).
- To avoid inconvenience and potential client dissatisfaction, be proactive:
    - Inform all affected parties of the COVID-19 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.
- Post signs at building entrance, person traps and high-traffic areas about sanitization and protective practices. Note that person traps could present a repository for the virus, in that they are small contained spaces, they are not usually ventilated, and they have surfaces that could allow the virus to live for hours, if not days. Clients should consider limiting the use of person traps and/or sanitizing after each use.
- Consider limiting the accessibility to shared spaces, such as client lounges, etc. Ensure there are sanitization supplies (and disposal units) in all shared areas, including next to vending machines.

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, access) for critical staff, and for critical facility exceptions to the general building rules, should be clearly identified to establish exception policies where appropriate.
- Operators should test all VPN connections to ensure reliable access, then instruct all staff noncritical to data center operations to access the systems remotely where possible.

12. Uptime Institute recommendations

In addition to the responses detailed above, Uptime Institute recommends organizations further consider the following:

Corporate response

- Stay current. Consult available information sources for updates and guidance.
- Share lessons. Because many organizations have data centers in multiple regions, responses may vary by location or facility characteristics. Share lessons learned in more affected regions with that less/not yet affected to strengthen their response.
- Secure documentation. Management may need to obtain permissions/official documents that permit key employees to travel to work (especially if cross-border commutes are common in the area).
- Clarify escalation process. Ensure that business units — especially mission-critical units — are fully briefed on response levels and the specific events that would trigger escalation.
- Ensure business/technical alignment. Encourage business unitscto be in frequent communication with data center operations and
- IT operations about policy changes that may impact data center/ IT operations. For example, directing employees to telecommute or instructing clients to use online services (similar to how some retailers have closed all of their physical retail stores and announced that their online store is still “open for business” this could drive a sharp increase in online traffic, for which IT should be prepared).

Data center response

- Review maintenance prioritization. Review maintenance plans and prioritize: Determine which tasks and issues can be downgraded/ responded to last or not at all if operating on a skeleton staff crew.
- Ensure good team communication. 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 system in advance.
- Avoid workspace sharing. Most data centers have limited workspaces for staff (e.g. BMS room, operations office, etc.).

- If possible, designate meeting rooms or other spaces for shift personnel 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 clean the shared spaces between shifts.
- Avoid equipment sharing. To the extent possible, avoid sharing equipment & provide each staff member his or her own resources.
- If equipment must be shared (e.g., shift phones, radios, tablets, tools, keyboards, etc.), sanitize at the start of each shift.
- Review external services. Increased telecommuting means increased stress on bandwidth, the power grid, networking, etc.
- Review and revise backup/disaster recovery plans as necessary.
- Make provisions for emergency housing. Although housing staff on-site should be considered only as a last resort, regions could go into lockdown mid-shift, so prepare for that eventuality:
    - Arrange with local authorities in advance for the data center to be designated as a critical facility (similar to a hospital or police station) and obtain permits for essential staff to travel. Explain the critical applications that the site supports (e.g., online banking, telecommuting, etc.).
    - Obtain supplies such as food, basic hygiene and medical supplies.
    - 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 and exercise facilities, etc.).

Review deferred maintenance

- Consider the consequences of deferred maintenance, as it may increase risk of component or system failure. As always, have a plan in place to respond to any major problem, coordinating with vendors as necessary, to ensure issues can be addressed.
- If equipment failure cannot be addressed in a timely manner, ensure procedures to address safe shutdown/isolation of the equipment and digital infrastructure is sufficiently resilient to absorb the loss of failed equipment (at least until workload can be transferred).
- As time passes and restrictions remain in place, revisit deferred tasks and determine whether continued delay increases risks beyond reasonable tolerances.

- Update core materials. While projects and maintenance activities are reduced, take advantage of the slower cycle to review and update plans and libraries (e.g., procedures, training content, skill inventories, plans for upgrades, succession plans). This can be accomplished off-site.
- Encourage documentation and knowledge transfer from experienced personnel; this could take the form of annotating procedures and manuals, video conferences between relevant parties, etc.
- Consider "recovered" staff both potentially infectious and at risk. Best information to date indicates 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.

13. Conclusions

COVID-19 has been active for many weeks (at the time of this report), but its impact on many organizations has been limited until recently. As a result, many businesses are (and will remain) in a reactive mode. Eventually this will be replaced by review and iterative improvement of policies and procedures; in the severity of the pandemic, it is likely that many of the policies will become permanently incorporated into critical facility management. This may increase overall costs. 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 COVID-19. This presents a challenge, given the existing and well-documented staffing shortages the industry faces. Current events reinforce the need for increased efforts on the part of the industry, educational institutions and trade organizations to strengthen recruitment and training programs. The current thinking is that the COVID-19 virus may become endemic (recurring on an annual basis, much like the flu. While dealing with the immediate challenges for the current global health crisis, business must also plan for the longer term. Business continuity plans should be updated to include prophylactic measures (e.g., requiring essential staff to be vaccinated at the start of each "flu season") and preparedness measures (reviewing digital resilience, site redundancy, vendor SLAs, etc.) as discussed in this advisory report. Uptime Institute will produce an advisory report for developing permanent processes/strategies as the lessons from this pandemic are learned.

BGD e-GOV CIRT

ICT Tower, E-14/X, Agargaon, Dhaka, Bangladesh

DIGITAL BANGLADESH
Skilled. Equipped. DigitalReady.

Bangladesh Computer Council

ICT DIVISION
FUTURE IS HERE

BGD e-GOV CIRT