



COVID-19

Pandemic Preparedness Plan

Risk Assessment Checklist for Your Business



With the coronavirus being a global concern, organizations need to be prepared for the economic fall-out and specifically, how to minimize the impact on their business. To that end, we provide a risk assessment list that organizations can use as guidance to prepare to deal with the effects of the coronavirus strain 19 and other future pandemics. While a full risk assessment and checklist will look different for each organization, we want to provide you with a structured starting point for questions you need to ask yourself and which sectors of your organization you need to consider.

Creation of a COVID-19 Incident Response Team

- Identify key personnel and create a COVID-19 Incident Response team who will coordinate the organizations effort.
 - This team should have representatives from HR, IT, purchasing, procurement, security, and legal with direct oversight from senior management.
- Ensure that the team creates a BCP (Business Continuity Plan) that considers relevant legal and regulatory obligations.
- Identify essential employees, those whose tasks cannot be performed by anyone else
 - Take steps to prevent these employees from getting sick in the first place, such as providing them with an alternate office to work from or allowing them to work remote as much as possible.
- Make sure that your team is documenting all decisions and steps taken in response to the outbreak, this is helpful in the event of possible future contract disputes or other legal matters arising from the effects COVID-19 has on your organization.

PUBLIC

Ecuron Inc. • 2929 Allen Parkway, Suite 200 • Houston, TX 77019 • 832.871.5970 • www.ecuron.com

Impact on Employees

- Prompt all employees to ensure that emergency contact information for them is up to date.
- Monitor the WHO and local government channels for advice and ensure that this information is distributed to your personnel.
- Introduce work policies to help enforce the isolation of staff, ideally enable the workforce to work remotely. If that isn't possible, consider the following:
 - Provide your staff with the right equipment such as soap, hand sanitizer, and masks (if recommended by local government).
 - Moving workstations so that staff have a distance of at least one meter between them.
 - Reducing the amount of personnel onsite to the essential staff only.
- Train and enable the workforce to work remotely, if possible. Ask yourself the following:
 - Can the employee's tasks be performed remotely?
 - Do they have a PC that allows them to work remotely?
 - If necessary, is a VPN (Virtual Private Network) client installed?
 - Is video conferencing software available on the PC?
- Create communication channels so that staff can inform the Incident Response team if they are sick or unwell.
- Introduce policies that limit business travel especially to high-risk areas
- Have back-ups readily available in case employees responsible for health and safety are unable to perform their roles.
- Provide the employees with information of where to get tested if they exhibit the symptoms of the coronavirus.

PUBLIC



- Consider implementing paid sick leave so that employees don't expose others to risk of infection if they are sick.

There are several companies offering free services to help companies work remotely during the COVID-19 pandemic. You can view services at <https://openforbusiness.org/>.

You may also need to consider legal issues related to your employees and the policies you enact for them. Things to consider:

- Whether employment terms permit periods of self-isolation (whether mandatory or self-imposed) to qualify as paid sick leave or as unpaid leave.
- Whether you have a right to require staff to work from home.
- Are you able to conduct voluntary or mandatory testing?
- Whether workers can be required to use annual leave for relevant absences.
- Will you allow requests for staff absence where a family member has the virus or is self-isolating (or if schools are closed or childcare arrangements impacted) and, if so, on what basis?
- Do you have a duty to inform/consult with health and safety representatives or works councils/trade unions in relation to the measures being taken?
- Whether you are eligible to apply for subsidies or financial support from national authorities if there is a business shutdown due to the virus, or a reduction in capacity due to sickness.

PUBLIC

Ecuron Inc. • 2929 Allen Parkway, Suite 200 • Houston, TX 77019 • 832.871.5970 • www.ecuron.com



Impact on Business

- Evaluate the potential implications for your customer and supply chain contracts.
- Review how COVID-19 will affect your ability to perform your contractual obligations (either directly or due to issues in your supply chain).
- Will any relevant Government response cause changes in law provisions?
- Do you have any notification obligations in relation to possible suspension or delays?
- Do you need to deal with supply chain insolvencies?
 - Is it viable to look to alternative suppliers or to agree to a commercial re-negotiation?
- Will financial statements be delayed?
- Are relevant parties (such as external auditors) able to access premises/information as needed?
- Will delivery of documents (such as financial reporting, operational certificates or waiver requests) be delayed due to employee absences?
- Is it necessary to disclose the impact on operations or any default?
- Is the company at risk of insolvency due to impact on revenues?
- Can any business interruption be claimed under existing insurance policies?
- Discuss with your brokers any possibility for coverage on new exposures.
- Logistics and costs involved with halting or altering normal business activities, for example a factory shutdown or site migration.
- Minimum staffing levels in order to maintain operations.
- Can on site tests and inspections still be performed?
- Ability to sign documents, specifically ones that require physical signing.

PUBLIC

Ecuron Inc. • 2929 Allen Parkway, Suite 200 • Houston, TX 77019 • 832.871.5970 • www.ecuron.com

IT and Cyber Security Concerns

- Inform employees that emails purporting to contain information about the coronavirus will only be coming from specific sources, remind them of their phishing training and of how to avoid phishing emails.
- Is there a need to add additional IT staffing in order to meet the increased IT needs of going remote, and if so where will the staffing come from?
- Ensure that systems are tested for resilience: can your systems handle the increased load if your entire work force goes remote?
- Can your IT team handle the influx of people needing technical assistance when moving to working remote?
- Does your IT team have a way to assist people who are working remote?
- Do you have a way to identify and contain the spread of malware on remote employee laptops?
- Ensure compliance with relevant data protection legislation.

In the EU, data concerning health is subject to enhanced protection under the GDPR (General Data Protection Regulation) as special category data. In the US, such data are subject to the HIPAA (Health Insurance Portability and Accountability Act) regulations.

Even if you are not in the health care business, information regarding employee's health, such as who has contracted the virus or not, may fall under this enhanced protection clause. Be sure that you are taking extra steps to protect this data so that your company isn't subject to fines.

PUBLIC



Communication

It is vital when dealing with disasters and a BCP that organizations keep open lines of communication, not just with their employees but with third parties who have a stake in the organization as well.

- Develop an emergency communication system for employees to keep them informed of what is going on with the company.
- Develop an emergency communication system for third parties who need to know what is going on with the company, such as suppliers, vendors, and investors.
- Keep employees updated with recommendations from the CDC and WHO.
- Consider any obligations to report on risks arising from (or the impact of) COVID-19 you might have.
- Consider how your organization will respond to stakeholder queries or press enquiries and whether you need to appoint a spokesperson and internal PR controls to manage this.

PUBLIC

Ecuron Inc. • 2929 Allen Parkway, Suite 200 • Houston, TX 77019 • 832.871.5970 • www.ecuron.com

APPENDIX

Current Cost of a Data Breach (Data as of July 2019)

| | |
|-------------------------------------|--------------------------------|
| Average cost of a breach worldwide: | \$3.92 million |
| Average cost in the United States: | \$8.19 million |
| Most expensive sector: | Healthcare with \$6.45 million |
| Average size of data breach: | 25,575 records |
| Average cost per record: | \$150 |

PCI Fines (companies dealing with credit card data):

- \$5,000 - \$100,000 per month, depending on size of business

HIPAA Fines (companies dealing with healthcare and medical records):

- \$100-\$50,000 per violation with a max penalty of \$1.5 million per year for violations that are identical.

Graham Leach Bailey Act (GLBA) (applies to financial institutions, not just banks):

- Up to \$100,000 per violation for the company
- Officers and directors can be fined up to \$10,000 per violation
- Also includes criminal penalties of up to 5 years in prison and the possibility of revocation of licenses

Sources:

- <https://www.ibm.com/security/data-breach>
- <https://www.lbmc.com/blog/pci-compliance-fees-fines-penalties/>
- <https://compliance-group.com/hipaa-fines-directory-year/>
- <https://www.shredit.com/en-us/blog/compliance/the-gramm-leach-bliley-act>
- <https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act>

About Ecuron

Ecuron is a boutique cybersecurity consulting company that specializes in preparing companies to face cyber threats. Our mission is to create a partnership with you, securing your data and protecting your organization every step of the way. For help developing and implementing an information- and cybersecurity strategy for your organization and for more information visit <https://www.ecuron.com> .

PUBLIC

Ecuron Inc. • 2929 Allen Parkway, Suite 200 • Houston, TX 77019 • 832.871.5970 • www.ecuron.com