

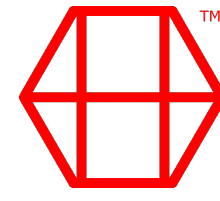
# Best Practice: Reducing Business Risk from COVID-19/Coronavirus

**List of countermeasures to reduce the impact of a pandemic on organisations**

v 0.2 - February 2020

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

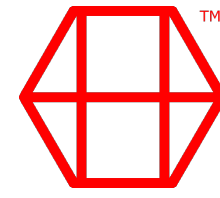


**“Health systems around the world are not ready!”**

– Dr. Mike Ryan, Head of WHO Emergency Health Programme

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in [#DigitalStrategy](#), [#CyberSecurity](#), [#CyberTerrorism](#), [#CyberDefence](#), [#CyberCrime](#)

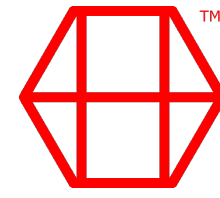


# About the Author

Lars Hilse works as an information security strategist for governments, and the private sector. For over two decades he was a member of a voluntary fire department, and acted as a battalion chief. During the course of his duty he was exposed to epidemic/pandemic trainings and methodologies.

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in [#DigitalStrategy](#), [#CyberSecurity](#), [#CyberTerrorism](#), [#CyberDefence](#), [#CyberCrime](#)

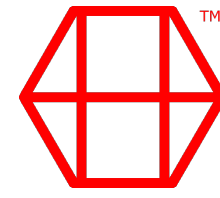


# About this Document

The risks of a pandemic are addressed in most responsible protocols in information security. This document is **a condensed list of countermeasures** to reduce the impact of a pandemic on an organisation all-together. It has been influenced by international best practice from a multitude of sources both practical, and theoretical.

[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

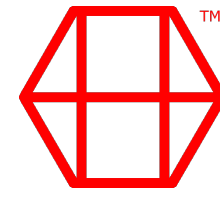


# Enabling Remote Work

Utmost priority is to prevent the virus from getting in // Amongst others, this can be achieved by complicating the spread in office spaces // All staff with remote work access need to stay clear of coworkers // Enabling a majority of staff to work remotely ASAP has highest priority

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

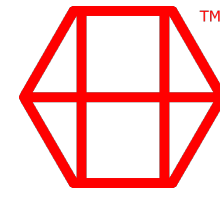


# Establishing Crisis Management Teams

The crisis management team is responsible for activating/deactivating the pandemic protocol // They also oversee the correct execution of the protocol during until protocol deactivation, and return to normal operations // Members should be representatives from executive level, work-/health safety, purchase, IT, asset management, union reps

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

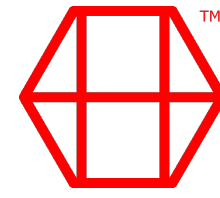


# Determining Core Business and Key Personnel

Determination limitation of business processes // Define criteria to business reestablishment after pandemic // Which processes may under no circumstances be interrupted; what is necessary to achieve this // Define core processes, key personnel, infrastructure personnel // Personnel for social aspects; social obligations // Remote work > Which staff can work from home

[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime



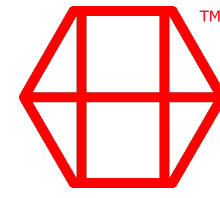
# Cooperations w/ Business Partners

Determining which products/services from partners are indispensable // Researching alternative providers of same/similar products/services // Determining which products/services the company has to provide to its clients // Agreements with contract staffers to temporarily replace infected workers

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime



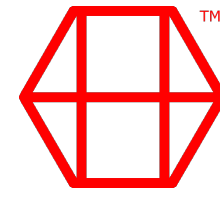


# Determining Business Units which can temporarily be shut down

Certain business units, which are not (as) profitable can be shut down temporarily //  
The risk of contamination by a resource in these BU is proportionately higher than  
closing the business unit down temporarily // Staff, which thereby becomes available  
is then integrated into more critical business units

**WWW.LARSHILSE.COM**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

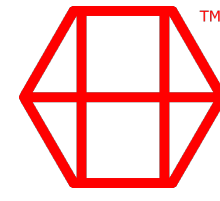


# Staff Care

Appoint crisis manager > coordinates measures concerning staff // Staff has to receive health advice, and looked after // Key personnel is to be isolated, and receives special attention in care, and prevention // Instituting a communication service > relays information between remote workers, and the company // Motivation in particular of key personnel // Medical officer leads efforts like vaccination, enlist additional medical staff, re-enlisting retired personnel with medical training, etc.

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

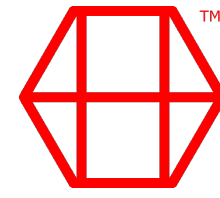


# Protection of the Business

Securing delivery/storage of critical resources // Factory/workplace security has to be upheld // Facility management has to be ensured // Ample supply of food, and safe drinking water // Ensuring trash collection, energy, functioning public transport and public health system // Assuming disruption in social life

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

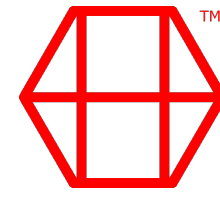


# Establishing Contact to Institutions outside of the Organisation

Energy suppliers, etc. // Establishing contacts to chambers of commerce // Creating a pandemic network w/ neighbouring businesses, the community, etc. to exchange information, collective procurement of supplies, etc.

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

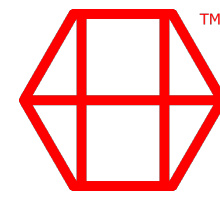


# Organising Care for Employees Abroad

Establishing contact with embassies/consulates // Premature recalling of employees abroad // Preparation for the pandemic in offices abroad // Organising backhaul of employees that have fallen ill, etc.

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

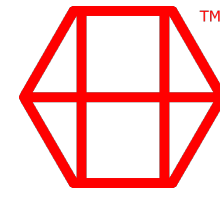


# Planning and procurement of medical- and sanitary/hygienic materials

Calculation of necessary materials // Researching correct materials // Respirators/  
masks // Gloves // Goggles // Further personal protection gear // Cleaning and  
disinfecting materials // Medication (antivirals, etc.) // Vaccination plans // Determining  
how materials are distributed // Establishing hygiene plans // Hand hygiene protocol //  
Paper towels to clean nose // Thermometers to measure temperature // Negotiating  
cost transfer with health insurances et al. // Procurement of antivirals through  
pharmacy/manufacturer // Seek permission to store within organisation

[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

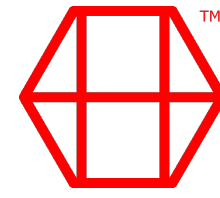


# Internal Information Policy

Development of a communication policy incl. crisis communication // When is the communication protocol activated // Role of the pandemic/crisis manager // Review possible multichannel delivery to employees to make information universally accessible // Pre-pandemic information delivery // Information policy during the pandemic, and after the pandemic is over // Educating staff about hygiene standards, and protocols // Information about medical treatment facilities, protocol when symptomatic, etc.

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime



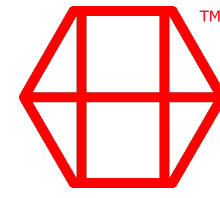
# Preparatory Medical Planning

Determining a medical practitioner (medical lead) // Planning and tasking of the organisations medical service // Planning required personnel // Acquiring additional personnel // Staffing reviews // Staff training in pandemic, hygienic principles, own responsibilities // Pandemic trainings // Determining lock-out of infected staff // Creating protocol if staff shows symptoms at the workplace // Prevention protocol through antivirals

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime



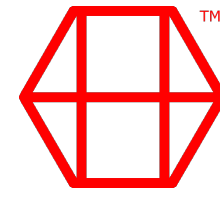


# Maintaining Minimal Operations

Crisis manager activates emergency response plan > informs organisations leadership, and staff // Activation of external staff, and resources // Adjustment of production // Shift of production to other sites // Activation of remote work // Adjusting communication to employees // Reduce personal contact of staff // Closing of uncritical business units // Data backups // Allday security for all sites // Deactivation of unnecessary staff // Reactivation of former staff // Install staff pickup service to avoid public transport

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

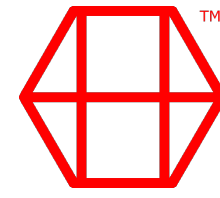


# Organisational Measures for Employees

Activation of key personnel // Supply of catering services, drinks, and food on site to avoid employees leaving site to eat // Supply enough personal protection gear // Advice on the correct usage of sanitary facilities // Continue use of air conditioning // Proper cleaning of the workplace // Personal hygiene training // Avoiding contact with other staff // Correct behaviour upon symptoms

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

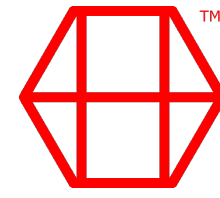


# External Information

Acquire continuous reports from government // Keep informed about therapeutics or vaccinations becoming available // Cooperate with pandemic network // Maintaining contact with customers // Acquire information about potential involvement into organisational sovereignty // Reporting infected staff.

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

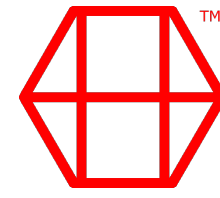


# Medical Measures

Limiting site access // Controlling movement of employees on site // Controlling personal meetings // Asking staff for their wellbeing upon arrival on site // If infection is suspected, lockout and sent to medical practitioner // Decontaminating everything infected staff has come into contact with // Secure usage of public places/interaction with customers // Separating entrance and exit // Provide staff with medication, and medical advice, personal hygiene advice, recommend vaccination (if available)

[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

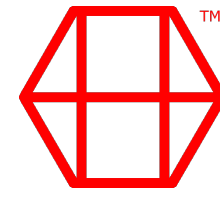


# Measures for Staff Abroad/Relatives

Retaining contact to unplanned absentees, deactivated employees // Provide information about domestic protective measures and behaviour // Offer support to relatives of infected staff // Supporting next-of-kin upon death of staff // If relative infected > offer housing for staff // Limiting travel to infection hotspots // Provide information about the condition in the home country of staff

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

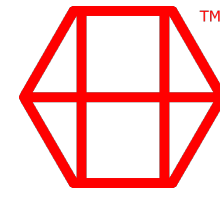


# Returning to Normal Operations

When the pandemic is over the crisis management team will restore conventional operations in the organisation by rolling back all previously mentioned measures in reverse order.

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in [#DigitalStrategy](#), [#CyberSecurity](#), [#CyberTerrorism](#), [#CyberDefence](#), [#CyberCrime](#)



# Contact Information

If you have further questions, and/or need assistance in implementing measures for the safety of your organisation please reach out now.

**Email** [lars.hilse@gmail.com](mailto:lars.hilse@gmail.com) (PGP Key ID 17FFC660)

**Phone** +49 (0)4835 9513027

**[WWW.LARSHILSE.COM](http://WWW.LARSHILSE.COM)**

Global Thought Leader in [#DigitalStrategy](#), [#CyberSecurity](#), [#CyberTerrorism](#), [#CyberDefence](#), [#CyberCrime](#)