Emergency Communications Plan

The Incom-CNS Group continue to closely monitor the coronavirus (COVID-19) outbreak in the UK. Our services remain uninterrupted and our core teams are working remotely to stay operational and on hand to provide support for our customers.

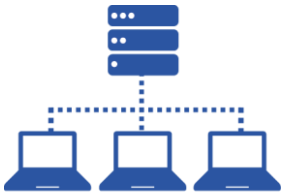
Further to a dedicated page on our website, set up to regularly update our customers on the latest measures we have in place, we wanted to share with you some useful tips for implementing an employee home working plan.

COMMUNICATION PLATFORMS

Check your business calls can easily be **diverted** to a home worker so you can continue to service your customers if employees are unable to get to the office.

VOICE AND DATA CONNECTIVITY

Remember if you can access your files remotely, maybe **cyber criminals** can too. Check your security is suitable.



IT AND NETWORKS

Audit employee's IT systems to make sure they are suitable. Laptops and mobile phones are likely the essentials, but also check for software updates and login details are correct.

If a significant or sustained event does occur, **additional hardware** may be required. Consider sourcing essential extra handsets etc. in advance to avoid any last-minute supply chain issues.

CLOUD SOLUTIONS

Is your key data easy to **access** if necessary? Think about where data is held either in the Cloud or on a server on site.

Are you still using physical **backup** storage and how will this continue if you can't access your equipment?

COLLABORATION SOLUTIONS

Does your business require people to meet and exchange ideas? Do you have a **virtual meeting facility** such as Mitel MiConnect or Gamma Horizon Collaborate?

Most Cloud based software used in the office should hopefully be easily accessible from home – those who don't regularly work from home may require **extra licences** however.

BUSINESS MOBILE

Employees can access data using their own devices, but this carries a greatly increased risk as it is far harder to track activity and prevent a **security breach**.

If connecting to the company network, strict policies need to be put in place to govern safe use and access.

Align your business continuity planning with your business communications

If a large scale sustained shut down occurs, quarantine measures may make access to premises very difficult.

Business Continuity Plans (BCPs) are vital for organisations to quickly become operational again when an incident or disaster strikes.

Business communications are essential to any successful BCP; without basic communications such as phone lines, it can be almost impossible to put into action your strategy or get other systems back up and operational.

Use this template to help ensure your business communications are firmly part of your BCP:

Identify key members of staff - Identify employees and senior management who are essential for daily operations and their deputies when away. Collect contact information for these people, including business phone (ext.), home, mobile, business email, personnel email and any other way of contacting them.

Redirects - Determine which numbers to set up redirects to if business phones or other communications are down.

Remote working – Enable staff members to work from home in an emergency. Ensure you have the systems in place to support this as part of your telephony system.

Create a directory of external contacts - List contact information for all essential suppliers, contractors, and service providers.

List all communications equipment - Create an inventory of all your communications equipment (phones, PCs, laptops, mobile devices etc.)

Assess back up processes - Make sure that there are robust back up processes in place for critical data relating to communications. The frequency of backups should be aligned with the importance of data to business operations.

Safekeeping of critical data - Your ability to enact disaster recovery and business continuity plans may depend on having access to certain data such as logins. For example, what information will you need to have to redirect phone calls to alternative numbers? This information must be kept securely and be accessible to key members of staff in an emergency.

Identify alternative supplies - If you are unable to access essential equipment such as phones or IT hardware, for example if your premises is out-of-bounds for some time, you may need to rent or purchase replacements. Have a list of suppliers that can meet your requirements at short notice.

Explore different scenarios - Different incidences will require a different response; make sure you've considered all possible scenarios. For example, connectivity issues or your building being inaccessible.

Create your Business Continuity Plan - As with your critical data, ensure all relevant information is kept in one document and that it is circulated to key members of staff. Also keep extra copies at a secure offsite location.

Test the plan - A Business Continuity Plan is worthless if you do not test it thoroughly. Review regularly changes to your organisation, such as migrating your business telephony from ISDN to SIP, moving to new premises, expansion etc. will have an impact on your BCP. Schedule regular reviews and always review and test after any significant changes.

Get in touch

Our team are experts in helping organisations work remotely and securely. If you are concerned about the impact on your business and require professional advice – please contact us on **0161 788 0000** or email **service@incom.co.uk** and we will be happy to help.