



Industry Security Notice

Number 2022/01

Subject: Business Continuity and Resilience

Introduction:

1. The aim of this Industry Security Notice (ISN) is to remind readers of the importance of having an effective and up-to-date Business Continuity Plan (BCP). This is essential to respond to incidents and be able to recover core activities should a disruption or multiple disruptions occur to your business as usual activities. This should include plans for critical ICT systems, along with appropriate arrangements to minimise the impact and can recover from a disruptive event.

Issue

2. It is crucial that everyone in industry is resilient to incidents that could impact Defence outputs and have a plan in place to respond when they arise. For instance, weather events, pandemic flu, terrorist attacks, denial of site or cyber-attacks.
3. If you have not planned for the 'what ifs', should something go wrong it's easy to tip into crisis and panic mode, then battle your way to get going again - which can be frustrating, stressful and impact Defence outputs.

Action by Industry

4. You have an important role to play and can do so by performing these basic steps:
5. Plan: if an incident happens, what's your plan B? Make sure you have thought about what incidents or disruptions you may encounter in your role/working environment, and have a plan so you know what to do if they ever happen. Your own personal plans should be a part of the specific BCP for your area. You should also ensure that you have confidence in your supply chain that they also have plans in place to protect continuity of supply in the event of a business continuity incident which interrupts their operations.
6. Prepare: test your plan regularly. If you haven't looked at your plan since before the pandemic, chances are it looks different now. But it's not enough to just 'have a

plan'. It should be tested regularly to see if it works and adjusted as needed. Remember, the best time to test your plan is before, not during a crisis.

7. Prevail: play your part to keep Defence operating. Everyone's role and work contribute to the defence of the UK – its crucial everyone can continue to play their part in the event of an incident. Having a backup and testing it regularly means we can face challenges confidently with minimal confusion or stress, and maintain outputs if something unexpected happens.

Validity / Expiry Date

This ISN is valid until further notice.

MOD Point of Contact

The point of contact in respect of this ISN is: COO-DSR-SyCommunications@mod.gov.uk