SECURE INNOVATION

AT A GLANCE: SECURITY FROM THE START

The following is a list of actions that your startup can take from day one in accordance with the guidance in Secure Innovation. They will reduce the likelihood of your startup falling victim to some of the more common attacks and will lay the foundations for strong security as your company grows.

Set the tone for a positive security culture:

- Develop a positive security culture through ongoing dialogue with all employees.
- Lead from the top by identifying a security lead at Board level.

Determine what you need to protect:

- Identify your most valuable assets which are critical to the existence and success of your business.
- Assess security risks and mitigations in conjunction with other risks to your business.
- Apply for the appropriate intellectual property protections for the jurisdictions in which you wish to operate.

Build security into your environment:

- Control access to your information and most valuable assets, with measures to detect unauthorised access, including:
  - Monitoring IT usage to ensure information is only accessed by those with a need-to-know.
  - Installing appropriate physical and virtual barriers such as safes, locks, strong passwords and encryption.
- Build in essential security measures when setting up your IT, including:
  - Deploying antivirus software and a firewall to protect your devices and internet connections.
  - Ensuring all software remains up-to-date, ideally using automated updates, and critical data is regularly backed up.
  - Enabling tools to track, lock or wipe lost or stolen mobile devices.
- Seek suppliers who provide security assurances suitable for your requirements.

CPNI Centre for the Protection of National Infrastructure

National Cyber Security Centre

SECURE INNOVATION

AT A GLANCE: SECURITY AS YOU GROW

As your company evolves and expands, managing your security remains an important factor to keep you on your trajectory to success. The following list of actions will help you identify and mitigate the additional risks that come with opening up to more partners and stakeholders.

As you increase collaboration, do so with security in mind:

- Take a strategic approach when considering how much data or proprietary information you must share with potential partners or investors.
- Where possible, use confidentiality agreements or NDAs as a tool to mitigate risk to information that you do share.
- Where possible, keep sensitive systems independent of those accessible by external parties.

As you expand internationally into new markets:

- Understand whether any new investment is likely to raise security concerns and consider security mitigation measures as part of your investment strategy.
- Check whether any products, software, or technology (including critical knowledge) that you wish to export are on the UK Strategic Exports Control List and apply for the appropriate licenses.
- Put in place proportionate and effective security procedures for any international travel.

As your team grows and you can no longer rely on personal relationships alone to build trust:

- Maintain your positive security culture through strong communication.
- Identify any roles that are exposed to higher risks and provide those individuals with additional support.
- Put in place a pre-employment screening process for all recruits into your business.
- Establish a security training package for staff, including at point of induction.

Minimise damage caused by a breach with a well-planned response:

- Establish and test an Incident Management plan.
- Detect and explore unexpected behaviour in IT and staff.

CPNI Centre for the Protection of National Infrastructure

National Cyber Security Centre