FIVE PRINCIPLES TO **SECURE INNOVATION**

1. KNOW THE THREATS

We want to support you to innovate and collaborate in a way that keeps your organisation safe and secure.

There are many ways a state-backed or hostile actor could try to get hold of innovations or technologies:

- **Insider**
- **Cyber**
- **Physical**
- **International Travel**
- **Investment**
- **Overseas jurisdictions**
- **Supply chain**

2. SECURE YOUR **BUSINESS ENVIRONMENT**

Effective protective security requires management of the security risks a business faces.

Ownership: Appoint a board-level security lead who factors security into business decisions and initiates a security dialogue within the business.

Identification: Identify your business-critical assets and the threats to them.

Assessment: Assess security risks alongside other risks to your business.

Mitigation: Protect your critical assets using physical and virtual barriers, access controls and detection and planning your response should something go wrong.

3. SECURE YOUR **PRODUCTS**

You should ensure the products and services your business is developing are secure, and that you are actively protecting and managing your intellectual assets and expertise.

Secure by default: Embed security in your products and services to keep your customers safe and develop a more secure society.

IP management: Identifying and actively managing intellectual assets, property and your business's expertise will help maintain the novelty and commercial value of your business's innovation.

4. SECURE YOUR **PARTNERSHIPS**

To operate securely, your company should manage the risks that partnerships with investors, suppliers and collaborators bring.

Background checks: Your business should know who you are working with.

Share with intent: Take a strategic approach to what you are sharing with partners, investors and potential investors.

Legal protections: Include protections for assets and data within contracts.

5. SECURE YOUR **GROWTH**

As your company grows, additional security risks arise which need to be managed.

Entering new markets: As you enter international markets, you will need to consider export controls, jurisdiction risk and travel security.

Expanding workforce: Growing companies will need to introduce pre-employment screening and security training, and work on developing or maintaining your security culture as your organisation changes.