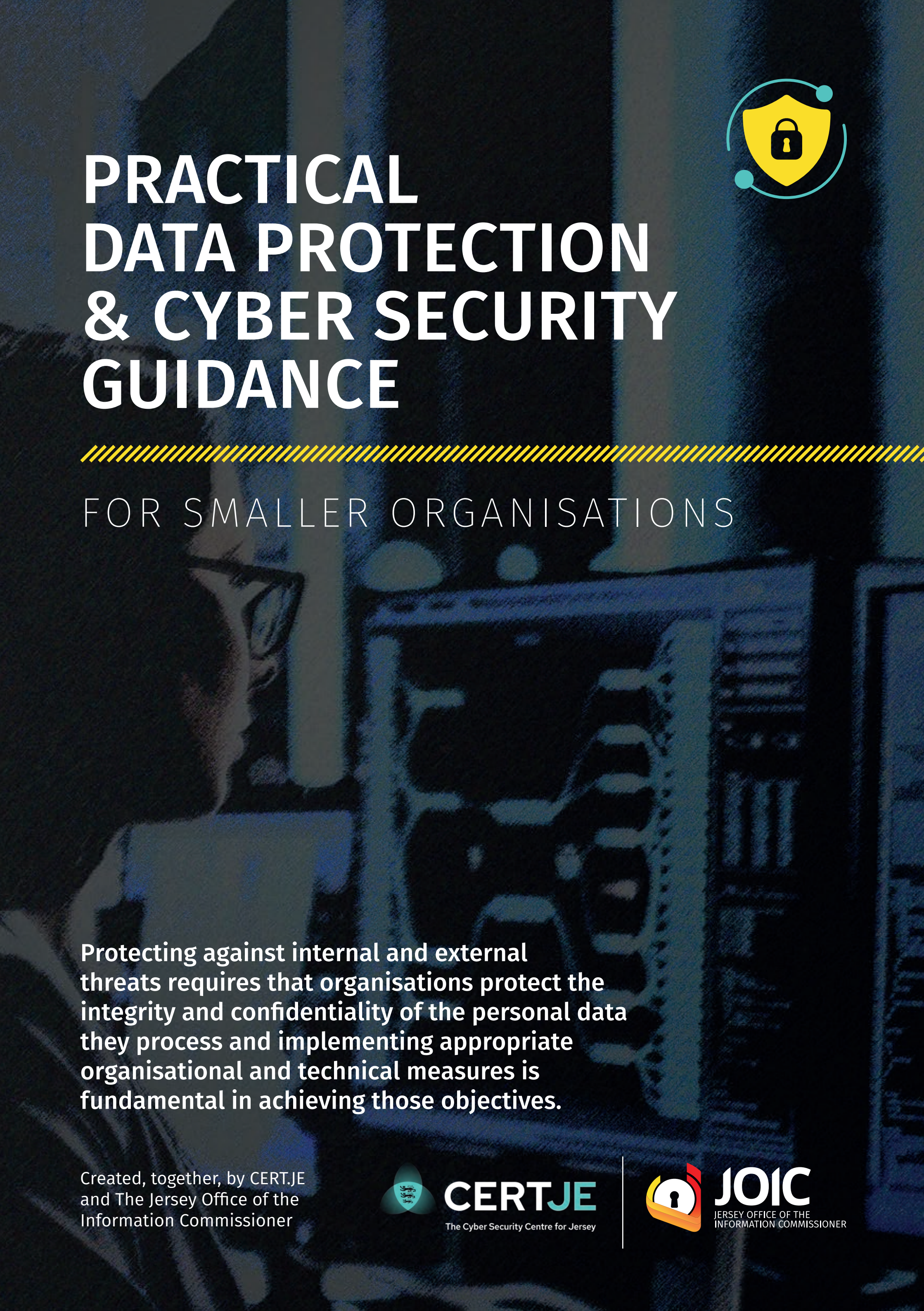
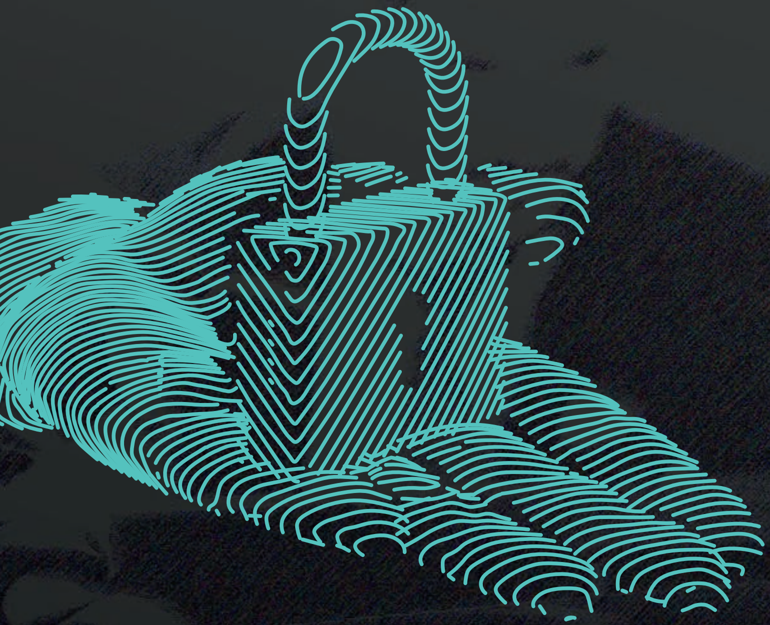


PRACTICAL DATA PROTECTION & CYBER SECURITY GUIDANCE

FOR SMALLER ORGANISATIONS

Protecting against internal and external threats requires that organisations protect the integrity and confidentiality of the personal data they process and implementing appropriate organisational and technical measures is fundamental in achieving those objectives.

Created, together, by CERT.JE and The Jersey Office of the Information Commissioner



Cyber attacks are hard to contain and can quickly impact any organisation - whether a target or not.

Inside this leaflet are some suggested practical organisational and technical measures that an organisation should consider to help protect the integrity and confidentiality of the personal data they process.

The leaflet also contains some basic but essential steps to reduce risk and ensure you can recover your organisation’s information if your network is compromised.

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.

→ TRAINING

Train, train, train. An appropriate level of data protection and security training and awareness for yourself, any and all staff, volunteers and executives is fundamental. All individuals with access to personal data need to be aware of what they can / cannot do with the information entrusted to them and what actions need to be taken if something happens. Appropriately trained staff are your first line of support and can help your organisation in maintaining the highest data protection standards and trust of clients and employees.

→ ACCESS

Access to both data and facilities should be given on the principle of least privilege. For example, access to systems, personal data, building workspace, filing cabinets etc. should only be provided to those who require access in order to complete the tasks they are required to. Access should not be given to just anyone and it should not be given on the basis of 'just in case', nor should everyone be given access to all systems and areas because it is easier to do so. This could place your organisation and its assets, including the personal data it processes at risk.

→ PATCH ALL YOUR SYSTEMS REGULARLY

In cyber security, a 'patch' is a fix - an immediate solution to an identified problem. Businesses and organisations should apply patches as soon as they become available. Patch your website, your databases, and infrastructure such as firewalls and routers. Linux servers, mobile devices, CCTV systems and IoT devices need to be updated too.

→ IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA)

Regardless of the system, a password should not be considered adequate on its own. Multi-factor authentication (or 2-step verification) is essential to protect user accounts and information.

→ CONTROL PRIVILEGED ACCESS

In addition to the customer and employee-facing systems you operate such as websites and email, you will have a lot of hidden infrastructure working hard for you. Admin accounts should be very carefully controlled, with rigorous use of MFA, careful access management, and a record of when an account is checked out for use, why and who by.

→ OPERATE EFFECTIVE MONITORING & ALERTING

It is essential to be the first to know when something goes wrong. That means logging the correct data and monitoring it for anomalies that suggest a problem. Monitoring doesn't have to be complicated or expensive. If you know which of your systems are critical, you can often outsource elements to a security supplier.

→ TEST YOUR INCIDENT MANAGEMENT PROCESSES

When the time comes and the worst happens, you can significantly reduce the impact by managing the incident well. The first step is to ensure you have an incident or crisis management plan. Who would do what, and when? Guidance is available from CERT.JE and online from the UK's NCSC.

→ MANAGE RISK IN YOUR VALUE CHAIN

You can't be completely responsible for your client's - or even your supplier's - security. However, you should recognise that the borders of your organisation are porous and take reasonable steps to reduce your risk.

→ SECURITY

Have you considered what measures you have in place to keep your organisation and its assets, including personal data, secure? Measures could include how the building is physically secured, if certain rooms such as server rooms have extra security and privileged access, how filing cabinets are locked and who has access etc. Security should also include management of others who may have access to your premises such as cleaners, visitors, clients, suppliers etc. It is extremely important to ensure you have undertaken relevant due diligence on your employees, suppliers, contractors etc. that you may be sharing or providing access to data or systems with.

→ MANAGE YOUR ATTACK SURFACE

Many attacks will start with a scan of your perimeter - this is everything someone without special access can see. You can do a lot to minimise this and make sure it looks boring to an attacker. If your network looks high risk and low reward, an opportunistic attacker will go elsewhere and a targeted attacker will find it harder to get in.

→ POLICIES & PROCEDURES

Having documented policies and procedures covering both data protection and information security is vital to ensure that the various processes and requirements have been captured so that all involved are aware and can refer to such, when necessary. Policies and procedures should be reviewed and audited frequently to ensure the controls and processes in place have been effectively implemented and are being followed as they should be. They should also be refreshed on a regular basis to ensure they truly reflect reality and include any updates when changes to any processes are made. It is also important to ensure you have a business continuity plan documented and access to back-ups in place in case something should go wrong.

→ VERIFY YOUR CONTROLS

Many successful attacks result from controls we intended to apply, but didn't fully — often because it was felt to be cost-prohibitive or inconvenient. Once you have implemented controls, make sure you know what exceptions you have — make them strictly time-limited, report them to the Board, and work over a few months to eliminate them.

→ MAINTAIN SEGREGATED BACKUPS

How long would you survive without your data? For most, it's not long. If data is available but corrupted, recovery is often even more difficult. Make sure your data is stored somewhere segregated from your primary network. This could be offline, such as a dedicated computer, storage array or USB stick. It could also be an online backup service or a cloud computing platform. Wherever you store it, remember to ensure that if usernames and passwords are compromised, they cannot be used to access and damage your backup data.

→ RETENTION & DESTRUCTION

A retention schedule is key to ensure you are not holding information, including personal data, for any longer than is necessary. A retention schedule should document the categories of data you hold and how long you are going to hold it for. If you have a retention schedule, are you following it and safely destroying data as and when required to do so? Many organisations have retention schedules but do not always comply with them. What method are you using to safely destroy the data? Is the destruction outsourced and have you checked the contractor process for safe destruction? How do you safely dispose of devices and electronic equipment that may hold personal data that you no longer require?

→ What happens if something goes wrong?

→ Can you identify if there has been a breach / incident?

→ How do you know if something has gone wrong?

→ Do your employees know how to identify and who to report to?

→ What is your plan if something has gone wrong?

→ Who can you contact for support, guidance and report to?

If the breach/incident includes personal data, know that the Jersey Office of the Information Commissioner is here to help, support and guide you. You may also be required to formally report the matter and if so, should do so within 72 hours after becoming aware of the matter if there is a risk to data subjects.

T: 01534 716530
www.jerseyoic.org/report-a-breach

JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

If it is a cyber security related incident, there's no need to be embarrassed. They happen all the time. However, by sharing we can protect others, and help ourselves in the future. Notify CERT.JE using the email address below so we can learn together as a community and stay one step ahead of the threat.

E: incidentreports@cert.je
www.cert.je

CERT JE
The Cyber Security Centre for Jersey

If the matter is crime related, for example concerning hacking or fraud etc, you may also wish to consider reporting to the States of Jersey Police.

T: 01534 612612 | www.report.jersey.police.uk

For the full content of this practical guidance, please visit **www.jerseyoic.org** or scan the QR code.