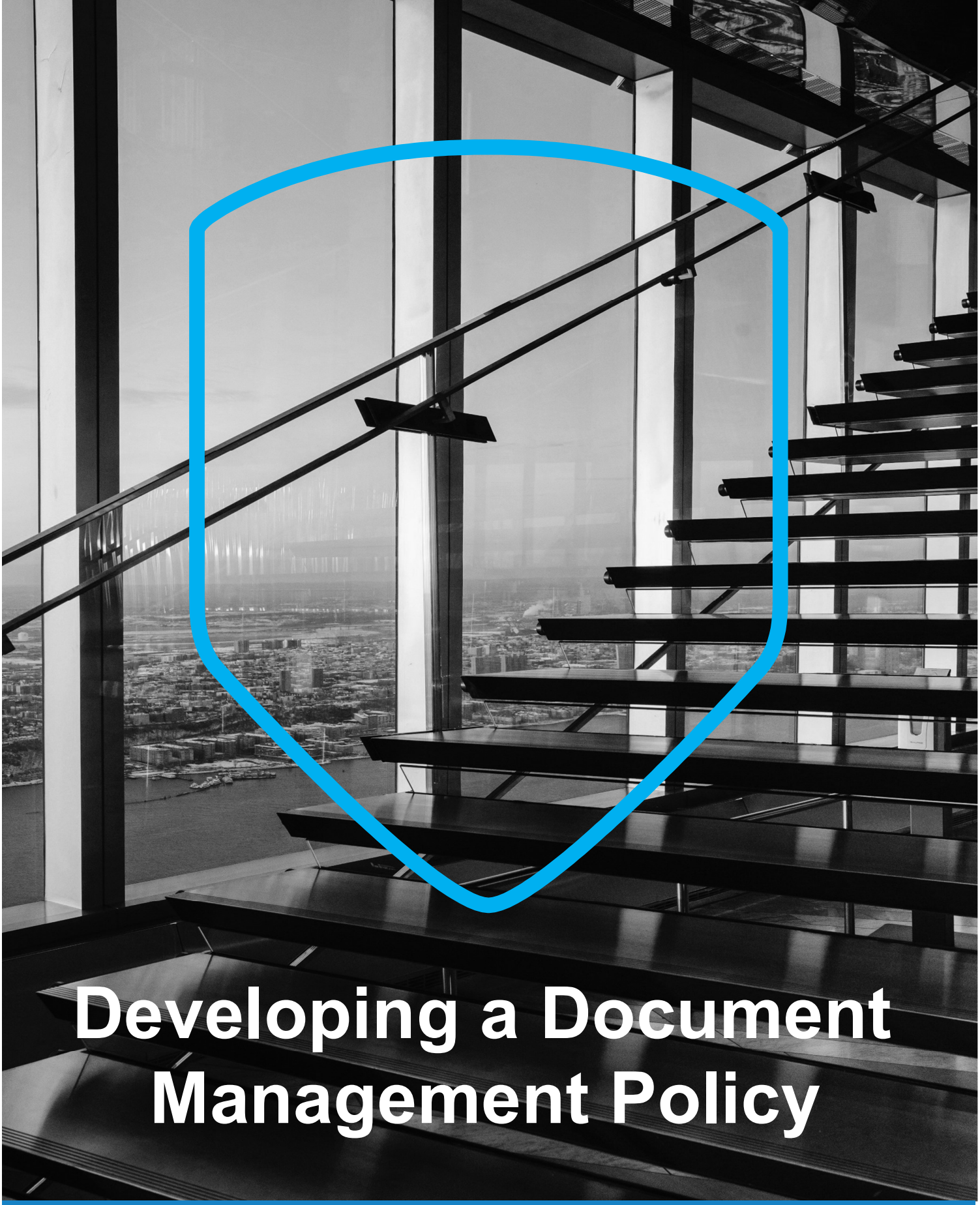
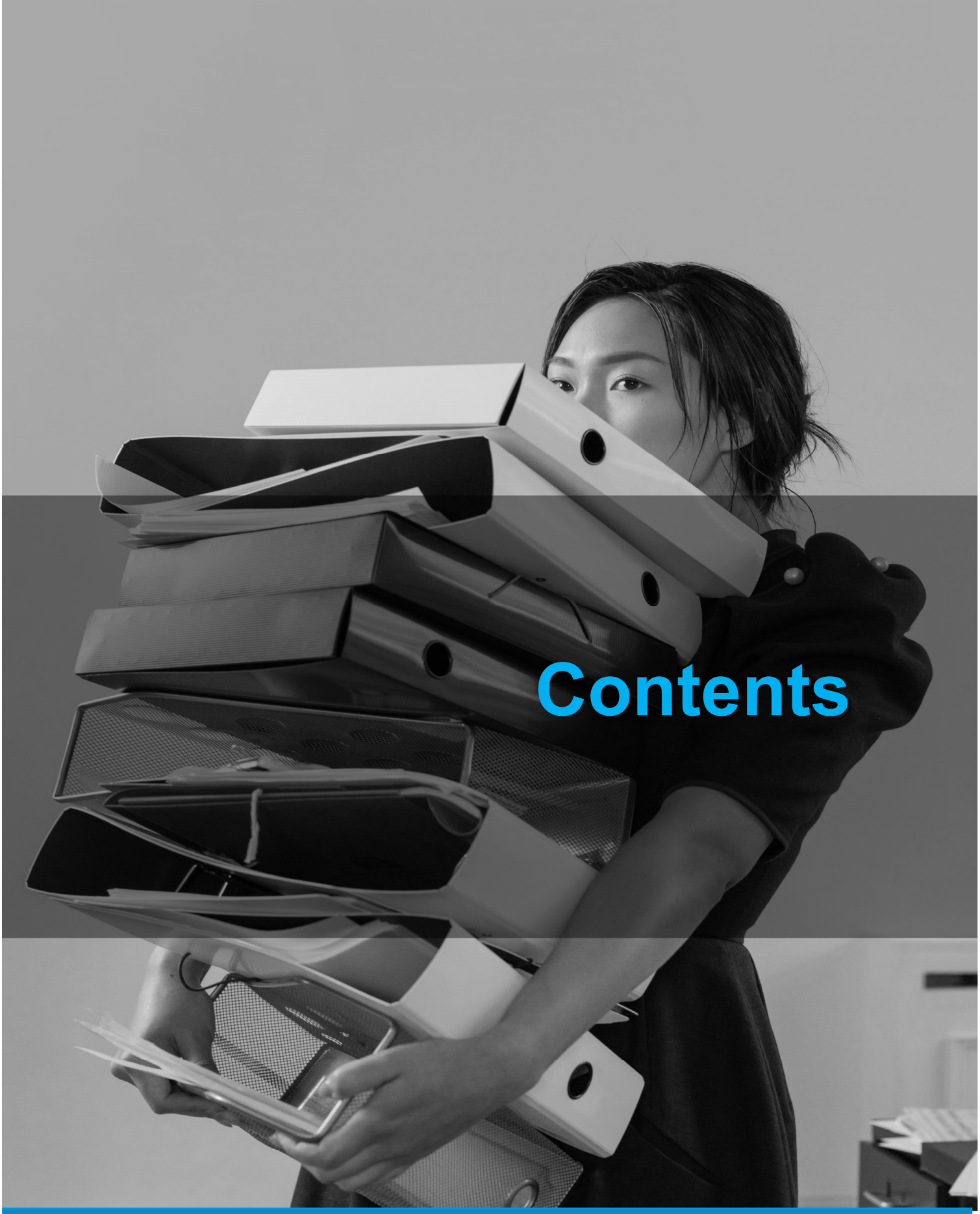


Developing a Document Management Policy

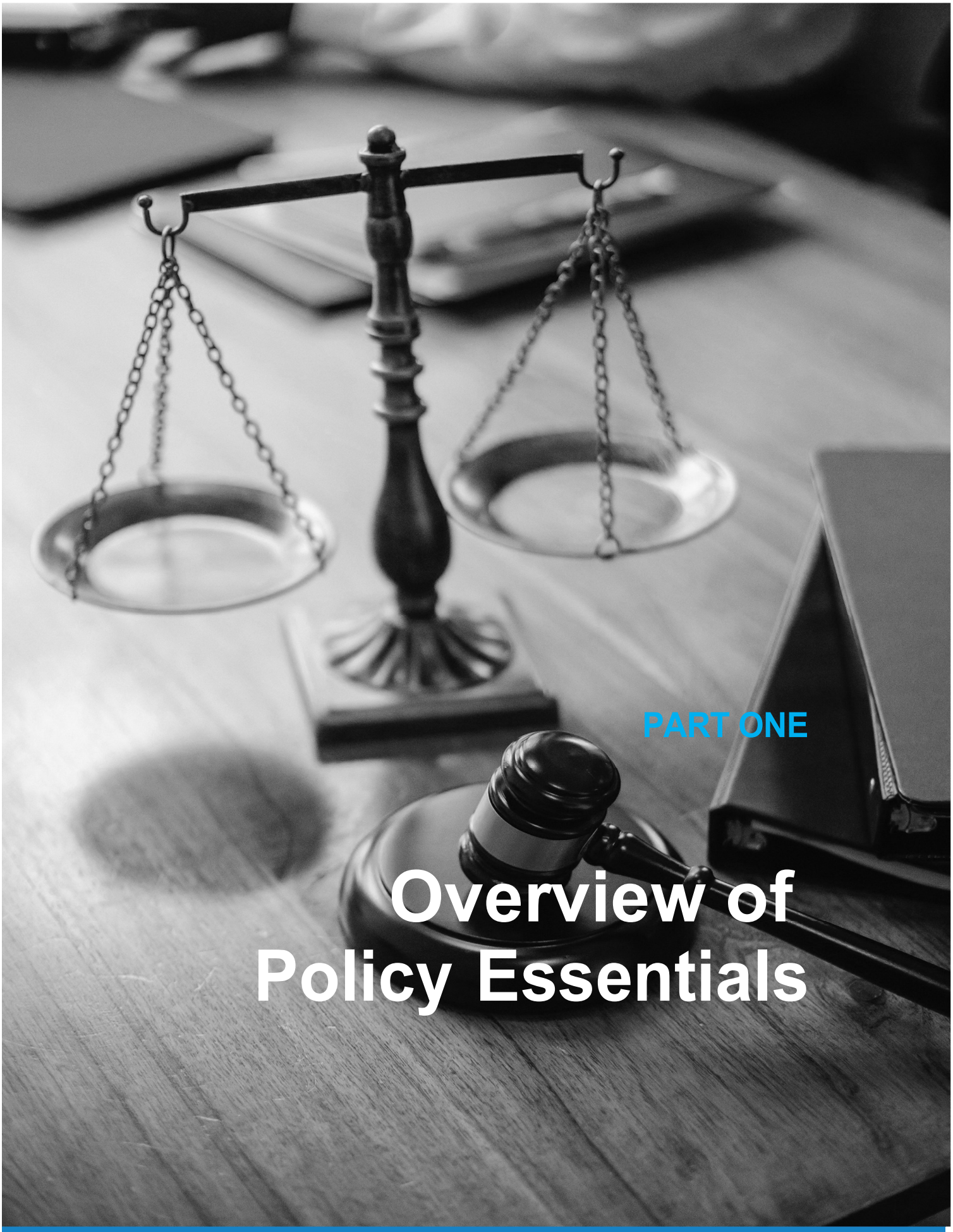
We protect what matters.

SHRED SAFE
DOCUMENT DATA DESTRUCTION & RECYCLING SERVICES



Contents

We protect what matters.



PART ONE

Overview of Policy Essentials

What policies or procedures do you have in place to deal with an employee who, even unintentionally, creates a potential identity theft opportunity? It could be as simple as leaving a document with confidential information on a desk or photocopier. Reduce your risk, create a clear and thorough Document Management Policy.

To start: Brainstorm your way to a good policy.

- Think about the kinds of situations that are likely to arise with your documents.
- Consider the implications of different actions and responses based on those situations.
- Decide who inside your organisation will be involved, and in what capacity.

Other questions to consider:

- Will there be any repercussions for employees who do not follow the procedures?
- Where (and how long) should each document be properly stored, and who in your organisation should have access to it?
- Will one employee within each department be in charge of maintaining information security and following up with fellow employees?

Consider these seven essential components of document management:

1. Changing confidentiality requirements

- Revisions to data protection law and government/regulatory body guidance make your document management policies and their proper use extremely important.
- Privacy laws include expensive penalties and fines for non-compliance.

2. Access to documents

- Protect sensitive information from unauthorised eyes inside and outside your organisation.
- Determine which documents contain confidential information, and where/how they're created.
- Inside your business, decide how sensitive each type of document is and determine who needs access to that information.

3. Document permissions

- Some personnel might be allowed to access a confidential document, but might not be allowed to change or remove it from its storage location.
- Provide read and write permissions. Only people concerned with creating and maintaining a document should be given both. Others would receive read-only permission.
- Determine and document who is in charge of filing or storing specific types of documents.
- Make sure that any contract or vendor personnel sign and adhere to confidentiality agreements as they affect documentation.

4. Document retention and destruction

- Establish specific guidelines that clearly identify the documents to be destroyed, and when, based on legal regulations that affect your business.
- Consider adopting a *ShredSafe All* Policy for any documents that aren't necessary to store. For help with this, see the ShredSafe Guide to Document Retention and the *ShredSafe All* Policy Guide at the shredsafe.net Resource Centre.
- Securely destroy your documents by using a professional destruction service that shreds the documents, and provides you with a Certificate of Destruction for auditable proof and protection.

5. Implementing your document policies

- Designate who will be responsible for ensuring that employees understand and follow through with the processes outlined in your policy.
- A logical choice may be the head of each department within your organisation.
- Expect that making changes will take time, so consider this a work in progress, and update or revise your processes as necessary.
- Enforcing the policy requires continually educating employees about why the policy is important, with step-by-step specifics.

6. Reviewing your document management policies

- Good document management requires a periodic review process that generates performance reports, which will show how well your organisation is carrying out the processes you've specified.
- Reviews are necessary to show authorities that your organisation is actually following regulations mandated by law and treating those regulations with respect. Part Three of this series will cover this area in more detail.

7. Labeling and storing your documents

- Information on paper requires a consistent labeling practice throughout your organisation to make it clear what a document is, along with its importance and when it can be securely destroyed.

More than 28% of information security breaches are caused by employee negligence.[1]

Surprisingly, the threat of a security breach is as likely to be inside your organisation than it is from the outside. That's because most breaches are caused by simple negligence and unintentional mistakes. When employees aren't sure how to handle documents, or they're unaware of the risks involved in throwing them in the waste or recycling bin, information breaches and the possibility of identity theft and fraud can happen. That's why we recommend a *ShredSafe All* Policy for every business. Once you no longer need documents for legal compliance or business reasons, don't store them – shred them, securely, with a reliable and professional shredding provider.

PART TWO

Best Practices for Implementing Your Document Management Policy

You've just outlined your basic policies for managing documents in your business. What's next?

Choose your leaders.

Whether your organisation is big or small, the only way to make sure that your new document policies work long-term is to stay on top of them.

- Choose a person in each area of your business who will be responsible for ensuring that employees understand and follow your new policies.
- The most logical choices may be the head or manager of each department in your organisation.
- Small office? Your office manager is the most logical person to supervise your new policies.
- Naturally, each person who supervises the new policies must also become a model for them, by following each policy to the letter.

Bring everyone together to announce your new policies.

- Include everyone in your business or organisation at your first meeting.
- Designate key speakers to outline your new document policies, step by step.
- Make sure the speakers explain why the policies are so important to the business (protecting confidential information, making documents easier to use and track, safeguarding business-sensitive information from your competition, clearing out and securely destroying documents when they're no longer needed).
- Make it an enjoyable event and encourage participation.
- Create a document that outlines the new policies to hand out to everyone.
- Leave plenty of time for questions and answers.

Hold smaller training meetings to put the policies into effect.

- For businesses with several departments and multiple employees, it helps to break policy training into smaller groups.
- Each leader should review the policies with his or her group, especially as the policies relate to specific documents within each department.
- Make sure employees understand that by following the new policies, they protect their organisation and themselves.
- Clearly explain any repercussions for multiple violations of the new policies.
- Answer any questions employees may have.

When it comes to managing documents, follow-through and consistency are the keys to success.

Once you've developed your document policies and everyone in your office knows what to do and follows through, working with documents will take less time. They'll also be easier to locate, update, file, discard and destroy at the appropriate times. And a less cluttered office space makes for a more productive business.

Keep the channels of communication open.

- People typically resist change, so expect that the new policies and procedures will take a few months to become habits.
- Meet within each department a month after the policies go into effect to find out how they're working.
- Ask for feedback from employees – you may be able to refine and make your policies better and easier to follow.
- If an employee slips up, an emailed reminder is all that's necessary, but make sure the employee is clear on what steps to take.
- The manager responsible for document security should record each document security infraction, to track how well your policies work.

Post reminders to make new processes easier.

- Hang posters or small signs in shared areas and wherever document processes take place: photocopiers, fax machines, filing cabinets, waste and recycle bins, and shredding consoles.
- Enforcing the policies you create requires a commitment to supervision until the new policies are habits for everyone in the office.
- Make sure that new employees receive training on your document policies.

PART THREE

Best Practices for Storing and Labeling Documents

What works for one business may not work for another, so put some time and thought into the best and simplest ways to keep your documents organised and secure. These guidelines are just that – use them as steps to create a storage and labeling system that keeps everyone in your workplace efficient and productive.

Provide document storage for every employee.

- Each employee should have at least one drawer to store documents off their desktop.
- Employees who handle confidential information should have file drawers they can lock.
- All sensitive information should be kept out of view of unauthorised personnel and locked up when not in use.

Determine each department's storage needs.

- For documents that multiple employees within each department will use, roughly determine how many filing cabinets you'll need.
- Allow for growth when choosing filing cabinets – documents accumulate quickly.
- Investing in storage that's large enough will reduce the number of times you have to re-sort and reorganise each department's filing system.

SHRED SAFE
DOCUMENT DATA DESTRUCTION & RECYCLING SERVICES

Develop a simple file-naming system that everyone can use.

- Clarity in labeling your files will save everyone time and trouble.
- Choose an alphabetical, numerical or subject naming system that will work best for your business, or a simplified combination of systems. Example: Client name / Job # / Date with year / Keep until (date/year).
- Be sure labels are legible. It may sound obvious, but misreading files can cause big mistakes.
- Invest in a label-making system that integrates with most popular word-processing software to keep your paper and electronic files in sync.

Consistency is the key to greater productivity in the workplace.

While most people have their own methods for organising and storing paperwork, it can be a big plus for any organisation to have one simple and consistent method for storing and labeling documents. When everyone follows the same system, it makes it easier to create, file and find important papers. In addition, by using the same system consistently, you'll know when it's time to discard and destroy the documents in your possession. By keeping documents secure at each stage of their lifecycle, you'll safeguard your business from the risks and expense involved in an information breach.

Clear out files regularly.

- Clear out old documents on a monthly basis to avoid clutter.
- Make sure all documents to be destroyed go into your locked consoles.
- Keep certain business and legal documents permanently – see the ShredSafe Guide for Document Retention for guidelines on how long to keep certain types of documents.

Use secure consoles to hold documents you no longer need.

- Keep confidential documents only as long as legally required.
- Once documents are ready to be destroyed, employees should dispose of them in securely locked consoles, preferably those from a professional shredding service provider.
- Place locked consoles in convenient, high-traffic areas around your workplace.
- For security reasons, documents should be securely shredded before they're recycled.
- A *ShredSafe® All* Policy can be the best way to help prevent security breaches.
- By shredding all documents, you avoid the risk of human error or poor judgment about which paperwork should be shredded.

SHRED SAFE
DOCUMENT DATA DESTRUCTION & RECYCLING SERVICES

PART FOUR

Reviewing Your Policy – Why and How Often

It's important to realise that every business, large or small, produces an extensive amount of sensitive information, ranging from customer lists and personnel records to account numbers and proprietary information about business operations.

While much of this information may also be electronic, a lot of it is paperwork that your employees handle every day. The only way to make sure your business is doing its best to maintain compliance is to periodically check how well everyone is complying with your new document management policies.

Conduct spot checks in addition to security audits.

- Each appointed department manager, security leader or office manager should track how well employees are following your new document processes, and record any infractions.
- Initially, you may want to track and report infractions on a monthly basis, then quarterly. Mistakes matter and could lead to an unintentional information breach.
- Follow up with those employees who may not understand how important your document policies are to maintaining security and compliance.
- Spot checks (checking without prior warning) within each department are a good idea, especially if you've recently hired any new employees.
- You should establish a schedule of when to conduct a full information security audit to review all your document policies.

Use your findings to review and update your document policies.

- Determine if there are specific areas or issues that are problematic.
- Review the correct procedures with everyone for any problematic areas.
- Revise policies as necessary to reflect changes to compliance laws.
- Post reminders about any changes to your document policies.
- Limit the number of employees who handle sensitive documents to help avoid internal security breaches.

Your document management policies are essential to keeping you in compliance.

The Privacy Act requires data controllers to ensure personal data is protected throughout its life, not kept for longer than necessary and destroyed securely at the end of its useful life. However, other legislation and regulatory guidance requires organisations to retain information for certain periods before securely destroying it. If a security breach occurs, non compliance with the relevant laws and regulations can result in severe penalties and fines for any organisation – not least of which is a monetary fine of up to a $1.7 million fine for serious breaches of the Privacy Principles (PPs).

The General Data Protection Regulation (GDPR) which will come into force in May 2018, and requires even more stringent data protection practices. With fines for non-compliance of up to 4% of global turnover or €20 million, it's vital to make sure your documents are secure at every stage of their lifecycle, including their destruction at the appropriate time.

Follow best practices to stay in compliance.

- Check often to make sure your business is in compliance with data protection legislation – see the shredsafe.net Resource Centre and check with your local regulators.
- Get help from legal professionals for complex areas of compliance.
- List all information security risks that affect your business, targeting both paper and electronic information sources, and review them periodically.
- Ensure that all your employees are in full compliance with legislation.
- Thoroughly train all employees about document security processes.
- Consider every stage of the information/document cycle, from creation and storage to how information is transferred and shared, through to the document destruction process.
- Outsource document destruction to information security experts who ensure the total security of the document disposal process.

SHRED SAFE
DOCUMENT DATA DESTRUCTION & RECYCLING SERVICES

How ShredSafe can help

ShredSafe associates are all Certified Information Security Professionals and provide advice and expertise to help you protect your business and stay up to date with changing privacy laws.

ShredSafe ensures materials are destroyed completely by your security-trained representatives. Upon completion, ShredSafe provides a Certificate of Destruction to confirm that the documents were destroyed.

For peace of mind, contact ShredSafe today on 02543355777 or visit us at shredsafe.net

Sources:
1. 2017 Ponemon Cost of a Data Breach Study: Global Overview

SHRED SAFE
DOCUMENT DATA DESTRUCTION & RECYCLING SERVICES