# SOC2 Policy Requirements

*Policies Saught by SOC2 Auditors*

TRUE NORTH

• PSR

# Table of Contents

## Policies List

- Information Security Policy
- Acceptable Use Policy (AuP)
- Business Continuity Policy (BCP)
- Disaster Recovery Policy (DRP)
- Incident Response (IR) Policy
- Code of Conduct (CoC) Policy
- Communications / Email Policy
- Backup & Retention Policy
- Physical Security Policy
- Risk Management Policy
- Data Classification Policy
- Access Control Policy
- Confidentiality Policy
- Workstation / Endpoint Security Policy
- Change Management Policy
- Logging & Monitoring Policy
- Password Policy
- Remote Access (Work From Home) Policy
- Software Development Lifecycle (SDLC) Policy
- Vendor Management Policy
- Encryption Policy

## Policy Summary Descriptions

### Information Security Policy

A high-level policy governing the approach to information security management within the organization. A required document for many security standards, including ISO 27001 and SOC2.

### Acceptable Use Policy (AP)

Describes the acceptable and prohibited uses of the organization's IT resources by employees or users to ensure security and compliance.

### Business Continuity (BC) Policy

This policy defines the processes and procedures employees must follow in case of a disruptive event to keep the business functions running smoothly. It also covers how the hardware, applications, and other crucial data will be restored in case of a disaster. Often, this policy is combined with the Disaster Recovery Policy (below).

## Disaster Recovery (DR) Policy

This policy defines the guidelines and instructions for the organization's recovery from a disastrous event. It outlines the core / critical functions your company needs to run its operations. Often, this policy is combined with the Business Continuity Policy (above).

## Incident Response (IR) Policy

A policy detailing the procedures and plans your company will use to respond to a security breach in accordance with applicable law. Most security and privacy standards (e.g., SOC2, ISO 27001) require this policy for effective incident management.

## Code of Conduct (CoC) Policy

Defines certain policies and procedures that employees and employers must adhere to. It includes how employees should interact with each other and define their expected behaviour toward colleagues, supervisors, and everyone else in the organization.

## Email / Communication Policy

Sets the guidelines for using the organization’s communication mediums. It mentions what is acceptable and unacceptable for employees when communicating using the company’s devices, networks, email, etc.

## Backup & Retention Policy

This document stipulates the criteria for determining how long data should be retained and the procedures for securely disposing of it once it is no longer needed.

## Physical Security Policy

Establishes measures to protect facilities, equipment, and resources from physical threats and environmental hazards, ensuring operational continuity and safety.

## Risk Management Policy

A crucial component of an organization's overall risk management strategy. It outlines the company's approach to identifying, assessing, managing, and monitoring risks.

## Data Classification Policy

Defines how to classify sensitive data by weighing the risk parameters. This ensures that the sensitive data is effectively handled according to the level of risk it poses to the organization.

## Access Control Policy

Establishes what measures you're taking to appropriately govern employee access to your company's various information and systems.

## Confidentiality Policy

This policy defines how your organization and employees will handle the confidential data of clients, business associates/partners, and/or the company itself. Clients expect the data you process or store on their behalf to remain secure, and this policy is an important part of ensuring that you deliver on that promise.

## Endpoint (Workstation) Security Policy

Defines rules and guidelines for securing the employees' workstations. This helps you reduce the risk of unauthorized access and data loss through workstation use.

## Change Management Policy

Establishes the process for managing changes to IT systems and infrastructure to minimize risk and disruption, and achieve repeatable success by using standardized workflows.

## Logging and Monitoring Policy

This document will list the log files you will collect and monitor. It also mentions what will be captured in those logs and what systems you must configure for logging.

## Password Policy

Defines the guidelines and requirements for using strong passwords (or passphrases). It mentions using password managers for different portals and includes a password expiration policy so employees regularly change passwords.

## Remote Access Policy

Provides guidelines and security measures for employees working remotely to maintain data security and productivity outside the office.

## Software Development Lifecycle (SDLC) Policy

Details how you will build your software/application using secure coding practices. Typically, this policy will also detail the testing procedures your Dev team will use to ensure your company's development workflows meet the compliance requirements.

### Vendor Management Policy

Sets security requirements and controls for third-party service providers ("suppliers", or "vendors") to protect your company's data and systems.

### Encryption Policy

Outlines the standards and practices for encrypting data to protect its confidentiality and integrity during storage and transmission.

## What Now?

As you've navigated through this guide, we hope you've gained a deeper understanding of the SOC2 requirements and the value those policies could add to your security program. Embracing SOC2 is not just about meeting a regulatory requirement; it's about securing trust in your services and protecting your customers' personal or otherwise confidential — a fundamental aspect of data-driven business.

At True North PSR, we recognize that the path to SOC2 compliance can seem daunting. If you determine you don’t have sufficient in-house resources to properly execute this project, this is where our expertise can make a crucial difference.

Our team is ready to assist you at every step, ensuring that your compliance efforts are as seamless and efficient as possible. By partnering with us, you gain access to a wealth of knowledge and a partner who is as committed to securing your systems as you are.

Consider visiting our website at <www.TrueNorthPSR.com> to learn more about how we can help streamline your compliance program, ease the burden on your internal teams, and enhance your security posture. We would be happy to help you turn the complexities of SOC2 compliance into a strategic advantage for your business.