# SUCCESS

## Security Democratized

**Secure Universal Creative Cost-saving Efficient Standards for Small Businesses**

**Ethical disclosure:** *Authors and University names are withheld due to research publication anonymity requirements. We plan and hope to add that information by the first half 2024.*

# Table of Contents

# Introduction

Security standards can be complex and costly to implement, posing challenges for small businesses with limited resources. This paper addresses these challenges by investigating the effectiveness of current security standards and proposing a novel framework tailored to the needs of Small and Medium-sized Businesses (SMBs). We present the Security Standards for Small Business (SUCCESS) framework, developed through a rigorous research methodology involving surveys, interviews, and field tests with SMBs. SUCCESS stands for **S**ecure **U**niversal **C**reative **C**ost-saving **E**fficient **S**tandards for **S**mall Businesses.

# Scope

The Security Standards for Small Business (SUCCESS) framework is designed to provide a streamlined and practical security standard tailored specifically to the unique operational environment and resource constraints of Small and Medium-sized Businesses (SMBs). This framework aims to address the complexities and financial burdens associated with conventional security standards, enabling SMBs to establish and maintain robust security practices effectively.

# Intended Audience

The intended audience for the standards aimed at small businesses encompasses owners, operators, and stakeholders of small-scale enterprises. This includes entrepreneurs, managers, and decision-makers who oversee the day-to-day operations and strategic direction of these businesses. Additionally, it extends to employees who play a role in implementing and adhering to the prescribed security measures. These standards are tailored to meet the specific needs, resources, and operational scope of small businesses, recognizing their distinct challenges and constraints. By addressing this audience, the standards aim to provide practical and accessible guidance to enhance security measures and protect sensitive information within the context of small business operations.

# SUCCESS Overview

Next, we present the SUCCESS overview table in two different versions

A. Standard Version, based on research and surveys
B. Beginners edition, very simplified language

After designing version A and improving the language of A for simplicity, we still got feedback that some business owners may not follow a few requirements. Rather than further simplifying, we created version B for beginners or those with little or no familiarity with security-related tasks.

The reason behind having different versions, A and B, is that while a few will need a very simplified version, the main version can still be useful by a security expert or auditor to help and guide a small business.

| SUCCESS Standards - Main Version | |
|---|---|
| **GOVERNANCE** | Leadership should provide support for security, including budget allocation |
| | Information Security Policy should be developed and implemented |
| **ACCESS CONTROL** | Strong password policies should be implemented. Along with a password (what you know), a second form of authentication (what you have) should be implemented. |
| | Access should be granted based on roles and responsibilities. Every employee should be granted the least possible access. |
| **ASSET MANAGEMENT** | Inventory of data should be compiled and maintained |
| | Data classification based on sensitivity should be performed |
| **DATA SECURITY** | Sensitive data should be encrypted |
| | Data leakage prevention should be ensured |
| **HUMAN RESOURCES** | Criminal Background checks for all employees and contractors should be performed. |
| | Job-specific training that addresses the unique security challenges shall be done annually |
| **SOFTWARE SECURITY** | Security should be integrated into every stage of the software development lifecycle |
| | Secure coding practices and code reviews should be implemented |
| **INCIDENT RESPONSE** | Develop a comprehensive incident response plan and test it |
| | Establish clear roles and protocols for reporting and escalating security incidents |
| **VULNERABILITY MANAGEMENT** | Ensure important updates for our computer systems are installed. |
| | Change passwords after any employee with sensitive data access leaves. |
| **RISK MANAGEMENT** | Potential risks and security weaknesses should be identified and assessed how they may harm. |
| | Plans should be developed to mitigate those risks |
| **PHYSICAL SECURITY** | Security measures to restrict physical access to sensitive areas should be implemented |
| | Comprehensive physical security policies should be developed to guide personnel and equipment protection |
| **TEAM** | An employee shall be designated to ensure above 20 guidelines are being followed |

# SUCCESS Standards - Beginners Version

| | |
|---|---|
| **GOVERNANCE** | Business owners should ensure security gets their attention and funds. |
| | There should be a document outlining security goals and priorities. |
| **ACCESS CONTROL** | Strong password policies should be implemented. Use a password (something you know) and a physical device like your phone (something you have) to access your online accounts. |
| | No more access or permissions to customer data should be provided than absolutely necessary. |
| **ASSET MANAGEMENT** | The location of all data, whether on-premise or on the cloud, should be understood and documented. |
| | Data of higher importance should be stored and processed with additional caution. |
| **DATA SECURITY** | Sensitive data like customer payment information or date of birth should be handled with extra precautions and converted to secret encoding (known as encryption). |
| | Please create awareness for all employees not to email customer information as attachments. |
| **HUMAN RESOURCES** | Criminal Background checks for all employees and contractors should be performed |
| | Job-specific training that addresses the unique security challenges shall be done annually |
| **SOFTWARE SECURITY** | If you write code or perform cloud computing, security best practices should be followed |
| | If you write code, secure coding practices and code reviews should be implemented |
| **INCIDENT RESPONSE** | Have a written Incident Response plan to perform actions in case of a data breach |
| | All employees and contractors should be made aware to report any data incident or breach. |
| **VULNERABILITY MANAGEMENT** | If you use any software tools, ensure to update to its latest version |
| | If your software or laptop provider sends important updates or instructions, follow those |
| **RISK MANAGEMENT** | Potential risks should be identified and assessed for various assets |
| | Take a backup of important data |
| **PHYSICAL SECURITY** | Security measures to restrict physical access to sensitive areas should be implemented |
| | Develop simple instructions and processes to ensure employees perform those |
| **TEAM** | Identify one employee to take responsibility for above 20 action items |

# Detailed Requirements and Guidelines

| Requirements and Guidelines | | Guidance |
|---|---|---|
| **Main Guideline** | **How to verify** | **Purpose:**<br>Support from leadership helps motivate all to care about security<br><br>**Best Practices:**<br>Allocate and document the budget for security.<br><br>**Examples:**<br>A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible and accountable. |
| 1-Leadership should provide support for security, including budget allocation. | 1A-Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and understood.<br>1B-Review budgetary allocation. | |
| **Challenges:** Small business owners or Founders may be juggling many things and may not have time to think about security<br>**Limitations:** Money for security improvements may be a low-priority<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>A documented Information Security Policy helps focus on a set of security priorities specific to the business.<br><br>**Best Practices:**<br>Do as you say, Say as you do.<br><br>**Examples:**<br>A template in English and Spanish is available at the accompanying website success4biz.info. |
| 2-Information Security Policy should be developed and implemented. | 2A-Review the Information Security Policy<br>2B-Interview a randomly selected employee about their understanding of the Information Security Policy. | |
| **Challenges:** Writing a formal security policy can be daunting, so start with a simple one-page about security problems and steps<br><br>**Limitations:** It may be tough without a template or example<br><br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | Guidance |
|---|---|

<table>
<tr><th>Main Guideline</th><th>Defined Testing Procedure</th><td rowspan="3">Purpose:<br>A documented Information Security Policy helps focus on a set of security priorities specific to the business.<br><br>Best Practices:<br>Set a minimum 10-character password<br><br>Examples:<br>NIST Multi factor guidance<br>https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication</td></tr>
<tr><td>3-Strong password policies should be implemented. Along with a password (what you know), a second form of authentication (what you have) should be implemented.</td><td>3A-Verify the existence of Two-factor access for all admins.<br>3B-Verify the adoption of two factors among randomly selected employees.</td></tr>
<tr><td colspan="2">Challenges: Setting up a two-factor can be a challenge.<br><br>Limitations: It may be impractical without smartphones.<br><br>Relevance: All types of Small Business</td></tr>
</table>

<table>
<tr><th colspan="2">Requirements and Testing Procedure</th><th>Guidance</th></tr>
<tr><td>Main Guideline</td><td>Defined Testing Procedure</td><td rowspan="3">Purpose:<br>Support from leadership helps motivate all to care about security<br><br>Best Practices:<br>Remove any access that is not needed when roles change<br><br>Examples:<br>Being added at the accompanying website success4biz.info.</td></tr>
<tr><td>4-Access should be granted based on roles and responsibilities to adhere to the principle of least privilege.</td><td>4A Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and understood.<br>4B Review budgetary allocation.</td></tr>
<tr><td colspan="2">Challenges: employees may have fast-changing roles<br>Limitations: removal of past role related permissions<br>Relevance: All types of Small Business</td></tr>
</table>

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Support from leadership helps motivate all to care about security<br><br>**Best Practices:**<br>Allocate and document budget for security.<br><br>**Examples:**<br>Being added at the accompanying website success4biz.info. |
| 5-Inventory of data should be compiled and maintained. | 5A Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and understood. | |
| **Challenges:** fast-changing scenarios<br>**Limitations:** Lack of data classification<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Proper data classification helps prioritize the security of highly sensitive data.<br><br>**Best Practices:**<br>Encrypt the highly sensitive data.<br><br>**Examples:**<br>Being added at the accompanying website success4biz.info. |
| 6-Data classification based on sensitivity should be performed | 6A Review Data Classification document<br>6B Review actual Data Classification | |
| **Challenges:** cost<br>**Limitations:** may not have many data types<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Encrypted data mitigates the risk of data theft in case of unauthorized access<br><br>**Best Practices:**<br><br>**Examples:**<br>Being added at the accompanying website success4biz.info. |
| 7-Sensitive data should be encrypted | 7A Verify encryption | |
| **Challenges:** expertise<br>**Limitations:**<br>**Relevance:** Small Business storing sensitive customer data | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>This reduces the risk of data loss and helps with legal compliance<br><br>**Best Practices:**<br>Begin by classifying your data into categories, such as sensitive, confidential, or public. This helps focus on protecting the most critical information.<br><br>**Examples:**<br>Customer personal information is classified as confidential. |
| 8-Data leakage prevention should be ensured. | 8A Interview personnel responsible for the implementation of Data Leakage prevention | |
| **Challenges:** selection of suitable tools<br>**Limitations:**<br>**Relevance:** Small Business storing sensitive customer data | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Promotes safe workplace and helps meet contractual obligations<br><br>**Best Practices:**<br>Reputable background check provider<br><br>**Examples:**<br>A list of background check providers shall be shared at success4biz.info |
| 9 - Criminal Background checks for all employees and contractors should be performed | 9A Review one randomly selected background check<br>9B Review the secure way of storing background check information. | |
| **Challenges:** cost<br>**Limitations:** basic background checks may not include all types of records<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Training helps reduce human errors and social engineering attacks<br><br>**Best Practices:**<br>Create a common minimum training first. Then develop for crucial roles.<br><br>**Examples:**<br>added to the website |
| 10 - Job-specific training that addresses the unique security challenges shall be done annually. | 10A Review different types of training materials<br>10B Review employee training evidence | |
| **Challenges:** prioritization by different departments<br>**Limitations:** not practical for very small business<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Security baked in early.<br><br>**Best Practices:**<br>Define security requirements early in the project, making them a part of the initial project plan and design.<br><br>**Examples:**<br>added to the website |
| 11 - Security should be integrated into every stage of the software development lifecycle | 11A Review different types of training materials | |
| **Challenges:** prioritization by different departments<br>**Limitations:** not practical for very small business<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Code review can prevent bigger problems later.<br><br>**Best Practices:**<br>Document the code reviews.<br><br>**Examples:**<br>May use a ticketing system. |
| 12 - Secure coding practices and code reviews should be implemented | 12A Review code review evidence | |
| **Challenges:** prioritization by different departments<br>**Limitations:** not practical for very small business<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>People understand their responsibility clearly.<br><br>**Best Practices:**<br>Create a very simple plan |
| 13 - Develop a comprehensive incident response plan and test it | 13A Review the Incident Response Plan | |

| | |
|---|---|
| **Challenges:** prioritization by different departments<br>**Limitations:** not practical for very small business<br>**Relevance:** All types of Small Business | first.<br><br>**Examples:**<br>added to the website |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Employees act fast during incidents.<br><br>**Best Practices:**<br>Conduct drills.<br><br>**Examples:**<br>added to the website |
| 14 - Establish clear roles and protocols for reporting and escalating security incidents | 14A Interview two employees | |
| **Challenges:** prioritization by different departments<br>**Limitations:** not practical for very small business<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Updates often patch for latest security updates.<br><br>**Best Practices:**<br>Update at least monthly.<br><br>**Examples:**<br>Being added to the website |
| 15 - Ensure important updates for our computer systems are installed | 15A Check for latest updates. | |
| **Challenges:** prioritization by different departments<br>**Limitations:** not practical for very small business<br>**Relevance:** All types of Small Business | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Updating software/following the given instructions maintain a higher baseline for security<br><br>**Best Practices:**<br>Update software with enforced frequency<br><br>**Examples:**<br>Enabling forced system-wide auto updates, mandating updates once a month |
| 16 - If your software or laptop provider sends important updates or instructions, follow those. | 16A Mainain software and hardware systems updated as per the manufacturer | |
| **Challenges:** Standardization of update procedure<br>**Limitations:** Lack of technical knowledge on where/how to do updates<br>**Relevance:** All types of small businesses | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Identifying risks and their impact can help mitigate their impact<br><br>**Best Practices:**<br>Develop privacy risk assessment to categorize sensitivity of and risk to different systems<br><br>**Examples:**<br>Being added to the website |
| 17 - Potential risks and security weaknesses should be identified and assessed how they may harm. | 17A Conduct system security audits<br>17B Maintain a record of breaches and known weaknesses to improve upon | |
| **Challenges:** Identification of all relevant risks<br>**Limitations:** Small businesses may not know how to identify all the risks<br>**Relevance:** All types of small businesses | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Having an outlined plan to mitigate risk will provide a standardized way to respond<br><br>**Best Practices:**<br>Create a minimum security policy first, and build upon it as the company grows<br><br>**Examples:**<br>NIST Framework gives a good outline, other resources on the website |
| 18 - Plans should be developed to mitigate those risks | 18A Develop security policy<br>18B Review and update security policy in a organization-defined timeframe | |
| **Challenges:** Developing policy that is simple but comprehensive<br>**Limitations:** Not practical for very small business<br>**Relevance:** All types of small businesses | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Protect data that isn't virtual/access to sensitive systems<br><br>**Best Practices:**<br>Develop and frequently update a set of physical security policies<br><br>**Examples:**<br>Locking file cabinets with sensitive data, putting keycard scanners at the entrances to sensitive areas |
| 19 - Security measures to restrict physical access to sensitive areas should be implemented | 19A Implement physical security measures to protect sensitive data | |
| **Challenges:** Cost of implementation<br>**Limitations:** Dependent on employees following secure policy (e.g. key storage)<br>**Relevance:** Any small businesses that aren't fully virtual (limited application as well to businesses that are) | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Develop a record of how to adhere to physical security guidelines and educate employees<br><br>**Best Practices:**<br>Train employees on physical security policies as they are modified<br><br>**Examples:**<br>Designating storage/use policy for employee key cards, secure storage policies for keys |
| 20 - Comprehensive physical security policies should be developed to guide personnel and equipment protection | 20A Train employees on proper use and implementation of physical security measures | |
| **Challenges:** Cost of implementation<br>**Limitations:** Dependent on employees following secure policy (e.g. key storage)<br>**Relevance:** Any small businesses that aren't fully virtual (limited application as well to businesses that are) | | |

| Requirements and Testing Procedure | | Guidance |
|---|---|---|
| **Main Guideline** | **Defined Testing Procedure** | **Purpose:**<br>Centralize security responsibility to reduce miscommunication and have someone who can resolve conflicts<br><br>**Best Practices:**<br>Pick an employee to run security who is well-versed in the policy and the systems of the business<br><br>**Examples:**<br>Head of Tech or IT |
| 21 - An employee shall be designated to ensure the above 20 guidelines are being followed | 21A Talk to the designated employee | |
| **Challenges:** Selection of employee<br>**Limitations:** No suitable employee may be available and willing<br>**Relevance:** All types of small businesses | | |

# Limitations

1. **Resource Constraints**: Small businesses typically have limited budgets and may not be able to allocate significant resources to implement and maintain robust security measures.
2. **Limited Expertise**: Small businesses may not have dedicated IT or security teams. As a result, employees with other responsibilities may be tasked with managing security, potentially leading to gaps in knowledge and expertise.
3. **Scalability Issues**: Some security standards may be designed with larger organizations in mind. Adapting these standards to fit the scale and scope of a small business can be challenging.
4. **Compliance Complexity**: Meeting certain security standards may require navigating complex compliance frameworks and legal requirements. Staying updated and compliant with evolving regulations can be difficult for small businesses with limited resources.
5. **Vendor and Supply Chain Risks**: Small businesses often rely on vendors and third-party services. Ensuring that these entities also adhere to security standards can be difficult, potentially exposing vulnerabilities.
6. **Balancing Usability and Security**: Implementing strict security measures can sometimes hinder user experience and productivity. Striking the right balance between security and usability is a challenge for businesses of all sizes.
7. **Limited Data Protection Resources**: Small businesses may not have the capacity to invest in advanced data protection technologies, potentially leaving them vulnerable to cyber threats.
8. **Target for Cyber Attacks**: Small businesses are not immune to cyber threats, but they might not have the same level of security infrastructure as larger enterprises. This can make them attractive targets for cybercriminals.
9. **Training and Awareness**: Ensuring all employees understand and follow security protocols can be challenging in a small business setting. Limited resources may hinder the ability to provide comprehensive training programs.

# Contacts

Since this work is part of ongoing research and is under consideration for publication; the actual contact information is anonymized for now. You can reach us at admin@success4biz.info or at (303) SUCCESS.