TERMS & CONDITIONS

Members shall not sell, distribute, rent, or lease in whole or in part to any third-party, copy, prepare derivative works based on, or publicly perform or display the policies and procedures. For further information, please read the terms and conditions below (also located on the My Wipfli membership website) before using Wipfli LLP's sample policies and procedures.

Wipfli Materials
License Agreement 20

SAMPLE ORGANIZATION

Technology and Risk Management
Policies and Procedures Manual

***<u>Editor's Note</u>*: The sample policies and templates included herein should only be used as a guide in developing policies and templates applicable to your particular organization. Users should carefully read the accompanying instructions and eliminate, add to, or modify these policies and procedures as necessary to customize them. These sample policies and templates are copyrighted materials of Wipfli LLP. My Wipfli members are authorized to use these materials only for the member's not-for-profit organization. Additional uses for multiple organizations or any other copying, reselling, or redistribution of these policies and templates is expressly prohibited.**

***<u>Editor's Note</u>*: If you currently use the manual and are reviewing a Wipfli LLP updated version (this version includes highlighted edits and additions to the text from the previous version), we recommend comparing your manual with the revised manual in its entirety, not just the highlighted areas. In some cases, portions of a policy or an entire policy may have been removed to bring the manual current, in these instances the changes may not be indicated.**

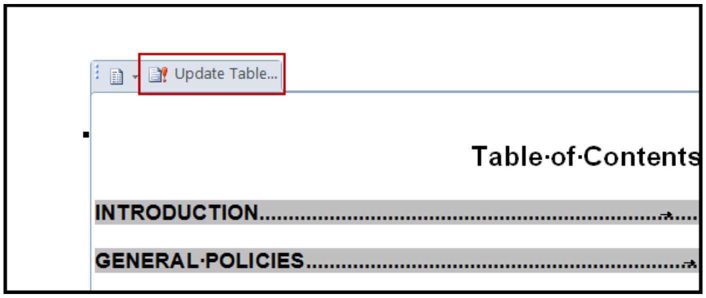
INSTRUCTIONS

TABLE OF CONTENTS – automatic

This document contains two types of Table of Contents (TOC); one that is automatically generated based on the document's formatted settings and another that is manually created. Please select the TOC that will work for your organization and delete the other.

If the automatic TOC is used, your Organization can edit or remove sample policies in this document and the TOC will update when the update button is clicked (see below). If the title/heading formatting of a policy section or individual policy is changed or removed, the automatic TOC will not generate properly. In this instance, please use correct the title/heading formatting or use the manual TOC and edit as appropriate.

To update the automatic TOC, click anywhere on the TOC near its top (see print screen below) and click on the Update Table button.

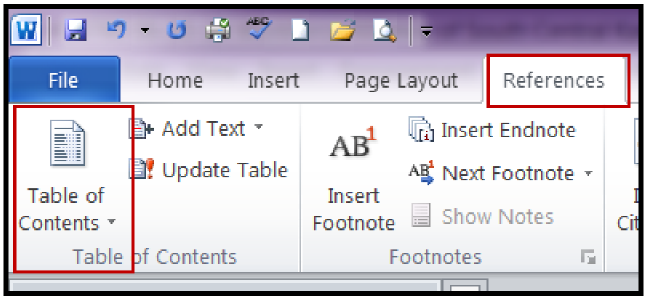


Table·of·Contents

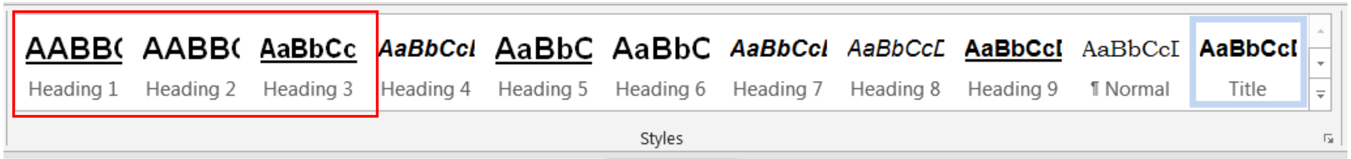
INTRODUCTION...

GENERAL·POLICIES..

The automatic TOC document is generated using the Microsoft Word Table of Contents feature located here:



If a heading is not included in the automatic TOC, on the Home tab of the ribbon, make sure the proper Style has been applied to the text.



HEADING 1

HEADING 2

Heading 3

TERMS & CONDITIONS I

INSTRUCTIONS I

TABLE OF CONTENTS – automatic i

TABLE OF CONTENTS – manual 9

ACCEPTABLE USE POLICY................................ ERROR! BOOKMARK NOT DEFINED.

OVERVIEW .... **Error! Bookmark not defined.**

Purpose and Scope .... **Error! Bookmark not defined.**

Acceptable Use of Organization Property .... **Error! Bookmark not defined.**

GENERAL REQUIREMENTS.. **Error! Bookmark not defined.**

INTERNET AND COMMUNICATIONS.................................. **Error! Bookmark not defined.**

CLASSIFICATION AND HANDLING OF INFORMATION....... **Error! Bookmark not defined.**

Information Classification Definitions .... **Error! Bookmark not defined.**

Information Owner Responsibilities................................... **Error! Bookmark not defined.**

Information Handling Table .... **Error! Bookmark not defined.**

E-MAIL COMMUNICATIONS .... **Error! Bookmark not defined.**

DOWNLOADS... **Error! Bookmark not defined.**

ACKNOWLEDGMENT SIGN-OFF... **Error! Bookmark not defined.**

DISCIPLINE FOR NONCOMPLIANCE.................................. **Error! Bookmark not defined.**

BUSINESS CONTINUITY PLANNING POLICY .... ERROR! BOOKMARK NOT DEFINED.

OVERVIEW .... **Error! Bookmark not defined.**

Authority .... **Error! Bookmark not defined.**

ASSET INVENTORY.. **Error! Bookmark not defined.**

Asset Identification... **Error! Bookmark not defined.**

RISK ASSESSMENT.. **Error! Bookmark not defined.**

Threat Scenarios .... **Error! Bookmark not defined.**

Severity and Likelihood... **Error! Bookmark not defined.**

PANDEMIC FLU.. **Error! Bookmark not defined.**

Pandemic Flu BCP Coordinator and BCP Committee Role **Error! Bookmark not defined.**

Limited Staff Planning... **Error! Bookmark not defined.**

OPERATIONAL REQUIREMENTS .... **Error! Bookmark not defined.**

Provisions.. **Error! Bookmark not defined.**

Facilities .... **Error! Bookmark not defined.**

Communication... **Error! Bookmark not defined.**

TRAINING .... **Error! Bookmark not defined.**

Training Levels .... **Error! Bookmark not defined.**

TESTING... **Error! Bookmark not defined.**

Test Plan .... **Error! Bookmark not defined.**

Test Types... **Error! Bookmark not defined.**

CLOUD SERVICES SECURITY POLICY .... ERROR! BOOKMARK NOT DEFINED.

OVERVIEW .... **Error! Bookmark not defined.**

CYBERSECURITY POLICY.................................. ERROR! BOOKMARK NOT DEFINED.

OVERVIEW .... **Error! Bookmark not defined.**

Cyber Risk Assessment and Remediation .... **Error! Bookmark not defined.**

Third Party Risk .... **Error! Bookmark not defined.**

- Web Site Risk .... **Error! Bookmark not defined.**
- Cyber Liability Insurance .... **Error! Bookmark not defined.**

DISASTER RECOVERY PLANNING POLICY ...... ERROR! BOOKMARK NOT DEFINED.

- OVERVIEW .... **Error! Bookmark not defined.**
  - Authority .... **Error! Bookmark not defined.**
- ASSET INVENTORY .... **Error! Bookmark not defined.**
  - Asset Identification .... **Error! Bookmark not defined.**
- BUSINESS IMPACT ANALYSIS .... **Error! Bookmark not defined.**
  - Prioritization .... **Error! Bookmark not defined.**
  - Recovery Time Objectives .... **Error! Bookmark not defined.**
  - Recovery Point Objectives .... **Error! Bookmark not defined.**
- OPERATIONAL REQUIREMENTS .... **Error! Bookmark not defined.**
  - Backup Use .... **Error! Bookmark not defined.**
  - Provisions .... **Error! Bookmark not defined.**
  - Facilities .... **Error! Bookmark not defined.**
  - Communication .... **Error! Bookmark not defined.**
  - Technology .... **Error! Bookmark not defined.**
- TRAINING .... **Error! Bookmark not defined.**
  - Training Levels .... **Error! Bookmark not defined.**
- TESTING .... **Error! Bookmark not defined.**
  - Test Plan .... **Error! Bookmark not defined.**
  - Test Types .... **Error! Bookmark not defined.**

DATA BACKUP POLICY .... ERROR! BOOKMARK NOT DEFINED.

- OVERVIEW .... **Error! Bookmark not defined.**
- ONSITE BACKUP .... **Error! Bookmark not defined.**
- EMPLOYEE LOCAL BACKUP .... **Error! Bookmark not defined.**
  - Data Replication .... **Error! Bookmark not defined.**
  - Offsite Backup .... **Error! Bookmark not defined.**
  - Backup Procedures .... **Error! Bookmark not defined.**
  - Data Backed Up .... **Error! Bookmark not defined.**

DIGITAL EQUIPMENT DISPOSAL POLICY .... ERROR! BOOKMARK NOT DEFINED.

- OVERVIEW .... **Error! Bookmark not defined.**
- DIGITAL EQUIPMENT DISPOSAL HANDLING REQUIREMENTS .... **Error! Bookmark not defined.**
  - Erasure and Destruction .... **Error! Bookmark not defined.**
  - Employee Purchase and Donation of Digital Equipment .... **Error! Bookmark not defined.**

DOCUMENT RETENTION POLICY .... ERROR! BOOKMARK NOT DEFINED.

- OVERVIEW .... **Error! Bookmark not defined.**
- POLICY .... **Error! Bookmark not defined.**
  - Document Types and Guidelines .... **Error! Bookmark not defined.**
  - Compliance .... **Error! Bookmark not defined.**
  - Exception for Investigations .... **Error! Bookmark not defined.**

INFORMATION SECURITY CONTROLS POLICY ERROR! BOOKMARK NOT DEFINED.

- OVERVIEW .... **Error! Bookmark not defined.**
- AUTHENTICATION AND PASSWORDS .... **Error! Bookmark not defined.**
  - Authentication .... **Error! Bookmark not defined.**

Passwords .... **Error! Bookmark not defined.**
NETWORK AND SYSTEM MANAGEMENT.......................... **Error! Bookmark not defined.**
Access Overview .... **Error! Bookmark not defined.**
Logging and Monitoring Reports .... **Error! Bookmark not defined.**
Patch Management.. **Error! Bookmark not defined.**
FIREWALLS AND VIRUS PROTECTION............................. **Error! Bookmark not defined.**
Firewalls .... **Error! Bookmark not defined.**
Virus Protection .... **Error! Bookmark not defined.**
OPERATING SYSTEM.. **Error! Bookmark not defined.**
System Hardening .... **Error! Bookmark not defined.**
REMOTE ACCESS .... **Error! Bookmark not defined.**
Employee Remote Access.. **Error! Bookmark not defined.**
Vendor Remote Access .... **Error! Bookmark not defined.**
PORTABLE MEDIA... **Error! Bookmark not defined.**
Laptops.. **Error! Bookmark not defined.**
Mobile Devices .... **Error! Bookmark not defined.**
Storage Media .... **Error! Bookmark not defined.**
INFORMATION SECURITY INCIDENT RESPONSE .... **Error! Bookmark not defined.**
Purpose .... **Error! Bookmark not defined.**
Incident Response Team .... **Error! Bookmark not defined.**
Incident Detection... **Error! Bookmark not defined.**
Incident Containment... **Error! Bookmark not defined.**
Incident Response Tracking Form Filing........................... **Error! Bookmark not defined.**
Client Notification... **Error! Bookmark not defined.**
Incident Resolution .... **Error! Bookmark not defined.**
Types of Incidents.. **Error! Bookmark not defined.**
ENCRYPTION.. **Error! Bookmark not defined.**
WIRELESS NETWORK SECURITY..................................... **Error! Bookmark not defined.**
Wireless Networks Connecting to the Organization .... **Error! Bookmark not defined.**
Procedures .... **Error! Bookmark not defined.**
Key Definitions... **Error! Bookmark not defined.**
General Responsibilities .... **Error! Bookmark not defined.**
Wireless Network Access .... **Error! Bookmark not defined.**
Audit and Monitoring Wireless Activity .... **Error! Bookmark not defined.**
Wireless Network/Device Security Requirements .... **Error! Bookmark not defined.**
Physical Security Requirements .... **Error! Bookmark not defined.**
Home Wireless Networks... **Error! Bookmark not defined.**
Documentation Requirements... **Error! Bookmark not defined.**
Related Organizational Policies/Forms .... **Error! Bookmark not defined.**
Applicability.. **Error! Bookmark not defined.**
CHANGE MANAGEMENT .... **Error! Bookmark not defined.**
Change Procedure Implementation.................................. **Error! Bookmark not defined.**
SOFTWARE INSTALLATION... **Error! Bookmark not defined.**
SOFTWARE LICENSING.. **Error! Bookmark not defined.**

INFORMATION SECURITY RESPONSIBILITIES POLICY .... ERROR! BOOKMARK NOT DEFINED.
OVERVIEW.. **Error! Bookmark not defined.**
RESPONSIBILITIES .... **Error! Bookmark not defined.**
Responsibility Objectives .... **Error! Bookmark not defined.**
Board of Directors/Governing Body................................... **Error! Bookmark not defined.**

Chief Information Officer .... **Error! Bookmark not defined.**
Information Technology/Network Manager......................... **Error! Bookmark not defined.**
Information Security Officer... **Error! Bookmark not defined.**
Personnel .... **Error! Bookmark not defined.**

INFORMATION SECURITY RISK MANAGEMENT POLICY.. ERROR! BOOKMARK NOT DEFINED.
OVERVIEW.. **Error! Bookmark not defined.**
POLICY.. **Error! Bookmark not defined.**
Risk Assessment .... **Error! Bookmark not defined.**
Risk Assessment Process .... **Error! Bookmark not defined.**

INFORMATION TECHNOLOGY AUDIT POLICY . ERROR! BOOKMARK NOT DEFINED.
OVERVIEW.. **Error! Bookmark not defined.**
POLICY.. **Error! Bookmark not defined.**
General.. **Error! Bookmark not defined.**
Information Technology Audit Responsibilities.................. **Error! Bookmark not defined.**

OPERATIONS POLICY... ERROR! BOOKMARK NOT DEFINED.
MANUAL/OPERATING PROCEDURES................................ **Error! Bookmark not defined.**
SEGREGATION OF DUTIES .... **Error! Bookmark not defined.**
Duty Categories.. **Error! Bookmark not defined.**
Duty Category Conflicts .... **Error! Bookmark not defined.**
Organization Department Responsibilities .... **Error! Bookmark not defined.**
Compensating Controls .... **Error! Bookmark not defined.**

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY..... ERROR! BOOKMARK NOT DEFINED.
OVERVIEW.. **Error! Bookmark not defined.**
SERVER ROOM .... **Error! Bookmark not defined.**
Heating/Cooling .... **Error! Bookmark not defined.**
Smoke Detectors .... **Error! Bookmark not defined.**
Fire Suppression... **Error! Bookmark not defined.**
Uninterruptible Power Supply (Ups) .... **Error! Bookmark not defined.**
Locks/Access.. **Error! Bookmark not defined.**
Wiring/Cabling .... **Error! Bookmark not defined.**
Flooring .... **Error! Bookmark not defined.**
Water Sensors... **Error! Bookmark not defined.**
DATA CENTER SECURITY .... **Error! Bookmark not defined.**
Access.. **Error! Bookmark not defined.**
Alarms .... **Error! Bookmark not defined.**
Cameras.. **Error! Bookmark not defined.**
Visitors.. **Error! Bookmark not defined.**
Packages/Shipping .... **Error! Bookmark not defined.**

SOCIAL MEDIA POLICY .... ERROR! BOOKMARK NOT DEFINED.
OVERVIEW.. **Error! Bookmark not defined.**
Purpose and Scope .... **Error! Bookmark not defined.**
Relevant Technologies .... **Error! Bookmark not defined.**
PROCEDURES... **Error! Bookmark not defined.**

DISCIPLINE FOR NONCOMPLIANCE................................ **Error! Bookmark not defined.**

SYSTEMS AND APPLICATIONS MANAGEMENT POLICY .. ERROR! BOOKMARK NOT DEFINED.
OWNERS/CUSTODIANS/USERS.. **Error! Bookmark not defined.**
Owner.. **Error! Bookmark not defined.**
Custodian .... **Error! Bookmark not defined.**
Users .... **Error! Bookmark not defined.**
ORGANIZATION FUNCTION.. **Error! Bookmark not defined.**
APPLICATION ATTRIBUTES IMPACTING NETWORK PERFORMANCE.. **Error! Bookmark not defined.**
Availability... **Error! Bookmark not defined.**
Deployment .... **Error! Bookmark not defined.**
Operational Workload .... **Error! Bookmark not defined.**
Integration... **Error! Bookmark not defined.**

SECURE SYSTEMS DEVELOPMENT POLICY.... ERROR! BOOKMARK NOT DEFINED.
OVERVIEW... **Error! Bookmark not defined.**
SPONSOR/OWNER REQUIREMENTS .... **Error! Bookmark not defined.**
Development Scope. .... **Error! Bookmark not defined.**
TESTING AND QUALITY .... **Error! Bookmark not defined.**
IMPLEMENTATION .... **Error! Bookmark not defined.**
SUPPORT AND MAINTENANCE... **Error! Bookmark not defined.**

TECHNOLOGY COMMITTEE POLICY OR CHARTER .... ERROR! BOOKMARK NOT DEFINED.
OVERVIEW... **Error! Bookmark not defined.**
Scope .... **Error! Bookmark not defined.**
Membership... **Error! Bookmark not defined.**
Program Oversight.. **Error! Bookmark not defined.**
TECHNOLOGY MANAGEMENT.. **Error! Bookmark not defined.**
Technology Governance and Board Updates .... **Error! Bookmark not defined.**
Business Continuity/Disaster Recovery .... **Error! Bookmark not defined.**
Vendor Management .... **Error! Bookmark not defined.**
Information Security.. **Error! Bookmark not defined.**
Systems (Network and Applications)................................ **Error! Bookmark not defined.**
MEETING PLANNING.. **Error! Bookmark not defined.**
Technology Committee Meeting Schedule Sample........... **Error! Bookmark not defined.**

TRAINING POLICY .... ERROR! BOOKMARK NOT DEFINED.
OVERVIEW... **Error! Bookmark not defined.**
TRAINING REQUIREMENTS... **Error! Bookmark not defined.**
Information Security Training .... **Error! Bookmark not defined.**
Technology Training .... **Error! Bookmark not defined.**
Regulatory Training .... **Error! Bookmark not defined.**
TRAINING SCHEDULE.. **Error! Bookmark not defined.**
Monthly Security Training .... **Error! Bookmark not defined.**
Additional Training Requests .... **Error! Bookmark not defined.**
PROGRAM MANAGEMENT RESPONSIBILITY .... **Error! Bookmark not defined.**

VENDOR MANAGEMENT POLICY...................... ERROR! BOOKMARK NOT DEFINED.
OVERVIEW... **Error! Bookmark not defined.**
VENDOR CLASSIFICATION.. **Error! Bookmark not defined.**
Vendor Criticality Risk Rating.. **Error! Bookmark not defined.**
VENDOR SELECTION AND CONTRACTING........................ **Error! Bookmark not defined.**
New Vendor Relationship Process.................................... **Error! Bookmark not defined.**
ONGOING VENDOR RISK EVALUATIONS:.......................... **Error! Bookmark not defined.**

CORPORATE AND PERSONALLY OWNED MOBILE DEVICE POLICY ....ERROR! BOOKMARK NOT DEFINED.
OVERVIEW... **Error! Bookmark not defined.**
POLICY.. **Error! Bookmark not defined.**
General.. **Error! Bookmark not defined.**
Organization Information Technology Responsibilities....... **Error! Bookmark not defined.**

TABLE OF CONTENTS – manual

	Page
Acceptable Use Policy	**1**
Overview	1
General Requirements	2
Internet and Communications	2
Classification and Handling of Information	4
E-mail Communications	6
Downloads	9
Acknowledgement Sign-Off	9
Discipline for Noncompliance	9
Business Continuity Planning Policy	**11**
Overview	12
Asset Inventory	12
Risk Assessment	12
Pandemic Flu	15
Operational Requirements	16
Training	18
Testing	19
Cloud Services Security Policy	**21**
Overview	21
Cybersecurity Policy	**23**
Overview	23
Cyber Risk Assessment and Remediation	23
Third Party Risk	24
Web Site Risk	24
Cyber Liability Insurance	25
Disaster Recovery Planning Policy	**26**
Overview	26
Asset Inventory	27
Business Impact Analysis	27
Operational Requirements	29
Training	34
Testing	34
Data Backup Policy	**36**
Overview	36

	Page
Onsite Backup	36
Employee Local Backup	36
Digital Equipment Disposal Policy	**39**
Overview	39
Digital Equipment Disposal Handling Requirements	40
Document Retention Policy	**43**
Overview	43
Policy	43
Information Security Controls Policy	**46**
Overview	46
Authentication and Passwords	46
Network and System Management	49
Firewalls and Virus Protection	53
Operating System	57
Remote Access	58
Portable Media	59
Information Security Incident Response	60
Encryption	64
Wireless	65
Change Management	73
Software Installation	73
Software Licensing	74
Information Security Responsibilities Policy	**75**
Overview	75
Responsibilities	75
Information Security Risk Management Policy	**79**
Overview	79
Policy	80
Information Technology Audit Policy	**83**
Overview	83
Policy	83
Operations Policy	**86**
Manual/Operating Procedures	86
Segregation of Duties	86

	Page
Physical and Environmental Security Policy	**89**
Overview	89
Server Room	89
Data Center Security	91
Social Media Policy	**93**
Overview	93
Procedures	93
Discipline for Noncompliance	95
Systems and Applications Management Policy	**96**
Owners/Custodians/Users	96
Organization Function	97
Application Attributes Impacting Network Performance	98
Systems Security Development Policy	**100**
Overview	100
Sponsor/Owner Requirements	100
Testing and Quality	102
Implementation	103
Support and Maintenance	103
Technology Committee Policy or Charter	**104**
Overview	104
Technology Management	105
Meeting Planning	106
Technology Projects Tracking (Sample)	107
Training Policy	**109**
Overview	109
Training Requirements	109
Training Schedule	110
Program Management Responsibility	110
Vendor Management Policy	**112**
Overview	112
Vendor Classification	112
Vendor Selection and Contracting	114
Ongoing Vendor Risk Evaluations	116
Corporate and Personally Owned Mobile Device Policy	**117**
Overview	117

	Page
Policy	117