

Security Policy

IDENTIFICATION AND AUTHENTICATION

THIS IS A COPYRIGHTED DOCUMENT.

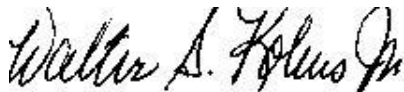
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your organization then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright permission. You will need to place the following documents in an envelope:

1. Fill out the Clearance Document and sign it; and
2. Fill out a check in the amount of five dollars, sign it, and make payable to TESS.

Send it to the following address: TESS, 1804 Small Ct, Raleigh NC 27612-3961. Please include your FAX number, if you have one and your mailing address so that I can send you a signed copy with both signatures.

If you are downloading multiple templates, you may include only one (1) Clearance Permission indicating the templates in paragraph 3, and a check made out in the total amount (templates X \$5.00).

Thank You,



Walter S. Kobus Jr, CISSP CISM NSA-IAM
Vice President Security Consulting Services
(919) 345-7449

CLEARANCE AGREEMENT

TESS will provide copyright license permission for use of TESS security templates (hereinafter called "Template") to _____ (hereinafter called "Recipient") for use in developing one copy of customized security documentation for the consideration of the sum of five dollars (\$5.00).

NOW, THEREFORE, in consideration of TESS Template, it is understood and agreed by and between RECIPIENT and TESS as follows:

1. **Adaptation Right.** RECIPIENT shall have the right to create an adaptation (called Derivative Works) of the Template. TESS copyright must appear on all adaptations to TESS Templates.
2. **Performance and Display Rights.** RECIPIENT may not display any TESS Templates in public in any media format.
3. **Exclusive or Nonexclusive.** RECIPIENT has nonexclusive permission of the following Template(s) _____

_____.
4. **Term of Use.** This Agreement, which is effective upon the date of its execution by the last of the signatory parties hereto, shall automatically expire and be deemed terminated effective upon the date of the happening or occurrence of any one of the following events or conditions, whichever shall first occur:
 - a. Mutual agreement of the parties to terminate the Agreement.
 - b. The expiration of a five (5) year period commencing on the effective date of this Agreement, unless such period is extended by mutual agreement of the parties in writing.
5. **Jurisdiction.** Jurisdiction of this agreement is in the State of North Carolina, United States of America. This Agreement is to be interpreted under the laws of the state of jurisdiction.
6. This Agreement shall inure to the benefit of and shall be binding upon both parties, its successors and assigns and shall be construed pursuant to the laws of the State of North Carolina, United States.

Total Enterprise Security Solutions, LLC
By: _____
Walter S. Kobus Jr., VP
Date: _____

Recipient
By: _____
Print Name: _____
Date: _____

Table of Contents

INTRODUCTION	5
REFERENCES.....	5
<i>Regulatory</i>	5
<i>Security Standards</i>	5
PURPOSE.....	5
SCOPE.....	5
SYSTEM ACCESS CONTROL SOLUTIONS.....	5
POLICY	5
COMPUTER LOGON	6
<i>Unique User Identification (ID)</i>	6
<i>Granting User IDs to Outsiders</i>	6
<i>Formats</i>	6
<i>Duplicate Logon IDs</i>	7
<i>User Agreement</i>	7
COMPUTER LOGON ID PASSWORD	7
PASSWORD STANDARDS	7
<i>User Authentication</i>	7
<i>Assignment of Passwords</i>	7
<i>Forced Change of All Passwords</i>	8
<i>Password Storage</i>	8
<i>Choosing Passwords</i>	8
<i>Logon IDs</i>	8
<i>Previous Password History File</i>	8
<i>Encryption of Passwords</i>	8
<i>Prevention of Password Retrieval</i>	8
<i>Reliance on Operating System User Authentication Process</i>	9
<i>Changing Vendor Default Passwords</i>	9
<i>Writing Passwords Down and Leaving Where Others Could Discover</i>	9
<i>Password Sharing Prohibition</i>	9
<i>Password Constraints</i>	9
<i>Disclosure of Incorrect Login Information</i>	9
<i>Prohibition of Multiple Simultaneous On-line Sessions</i>	9
<i>Automatic Log-Off Process</i>	10
COMPUTER LOGON ID SUSPENSIONS AND CANCELLATIONS	10
<i>Inactivity</i>	10
<i>Misuse</i>	10
TERMINATION OR REASSIGNMENT OF A COMPUTER LOGON ID.....	10
<i>Termination</i>	10
<i>Multiple User Logon IDs</i>	10
OPERATING SYSTEM SECURITY FEATURES.....	11
<i>Processing Financial Information</i>	11
<i>Browser Warning Logon Banner</i>	11
<i>Financial Information Segregation</i>	11
<i>Emergency and Temporary Access</i>	11
<i>Tokens</i>	11
<i>Clock Synchronization</i>	11
<i>Remote Access</i>	11
<i>Data Files and Software Logical Control</i>	12
<i>Database and DBMS Logical Controls</i>	13
RATIONALE	13
RISK	13

IMPACT	13
<i>Users</i>	13
<i>Data Owners</i>	14
<i>Managers</i>	14
<i>Application Development and Database Administrators</i>	14
<i>Access Control Team</i>	14

Introduction

References

Regulatory

Insert regulatory such as Sarbanes-Oxley, HIPAA, G-B-L etc.

Security Standards

1. ISO 15408-2, Common Criteria, paragraph 7, Class FIA: Identification and Authentication.
2. ISO 15408-2, Common Criteria, paragraph 12, Class FTA: TOE Access.
3. International Standard, Information Technology – Code of Practice for Information Security Management, ISO/IEC 17799:2000(E), paragraph 9, Access Control.
4. DoD Directive 5200.28, Trusted Computer System Evaluation Criteria, C2 Class Assurance Level.

Purpose

The purpose of this policy is to establish for the [ORGANIZATION] a policy on the use and deployment of a variety of access control solutions to ensure the confidentiality, integrity, and availability of the [ORGANIZATION]'s information assets. This policy is to maintain an adequate level of security to protect the [ORGANIZATION] data, financial data, and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection, and to ensure a secure and reliable operation of the [ORGANIZATION]'s information systems. This policy applies to all computers and communication systems, owned or operated, by the [ORGANIZATION] and its subsidiaries. Similarly, this policy applies to all platforms, operating systems, and applications.

Scope

This policy illustrates the need for access control software to be an integral part of the [ORGANIZATION]'s information systems management program. The policy is to set forth mitigation controls to allow for the authorized access, while maintaining an adequate level of security in protecting the [ORGANIZATION]'s informational data. For the purpose of this policy, these types of controls shall be referred to as “system access control solutions.”

System Access Control Solutions

Policy

Access to the [ORGANIZATION]'s information assets will be granted on different levels, based on the business rules established by data owner's of that information, for an authorized user or entity to create, read, update, delete or transmit that information. Users will be provided access based on the concept of “least privilege.” Access will be managed and controlled through discretionary access controls, identification and authentication, and audit trails.

Use of the [ORGANIZATION]'s information assets shall be restricted and shall be allowed only as necessary to support authorized business activities. The business rules currently in effect in conjunction with the [ORGANIZATION]'s user-based access controls shall be reviewed for adequate security level access and protection, and may serve as the foundation for establishing compliance with this policy.

Any effort to circumvent the [ORGANIZATION]'s information security mechanisms to gain access or to exploit any known or unknown vulnerabilities shall be perceived as a security incident, and shall be handled in accordance with established incident reporting guidelines and/or appropriate human resources policies and procedures.

All of the [ORGANIZATION] information is considered an asset and is protected, in all of its forms, from accidental or intentional but unauthorized, disclosure (confidentiality), modification or destruction (integrity), or the inability to process that information (availability).

Computer Logon

The [ORGANIZATION] shall take appropriate action to ensure that all full-time associates, regular part-time associates, agents, contractors, consultants, temporary associates and all other non-associates must use Unique User IDs and passwords to gain authorized access to any of the [ORGANIZATION]'s information assets.

Unique User Identification (ID)

Each authorized user shall be assigned a Unique User ID for which that user shall be held responsible and accountable for the purpose of initiating the login process to the [ORGANIZATION]'s information systems. The Unique User IDs are not to be shared with other users for the purpose of gaining access to the [ORGANIZATION]'s information assets. Authorized users shall be held accountable and responsible for the use and activity of assigned Unique User ID.

Granting User IDs to Outsiders

Individuals who are not employees, contractors, or consultants must not be granted a User ID or otherwise be given privileges to use the [ORGANIZATION] computer resources or communications systems unless the advance written approval of a department head and has been obtained and the appropriate agreements, clearance and access forms have been accomplished.

Formats

Computer logon ID formats and lengths are governed by the host system or software constraints. Generally, computer logon IDs fall into three categories, mainframe logon ID, and mini, micro and/or LAN logon IDs.

1. Mainframe logon IDs. Naming standards facilitate identification of users or computer-to-computer linkage. The minimum length of a mainframe logon ID shall be at least six characters.

2. Mini, Micro and/or LAN Logon IDs. These logon IDs are designed to facilitate easy identification for user-to-user type communication. The format of the logon ID is based on the user's first name initial, middle initial, and last name. The minimum logon ID length shall be eight positions. Position one consists of the first initial of the user's first name. Position two consists of the first initial of the user's middle name. If the user does not have a middle name or initial, this position is filled with the letter "X." The final six positions consist of the first six letters of the user's last name. If the user's last name is shorter than six letters, the remaining positions up to position six are filled with unique consecutive numeric digits starting with 01. This standard applies throughout the [ORGANIZATION], unless technically prohibited by the operating system. Exceptions to these standards must be requested in writing, stating the reasons an exception is needed. Send the requests to the Information Security Officer. However, logon IDs that do not conform to these standards, but were in existence before issuance of these standards, are not required to change.

Duplicate Logon IDs

No two users within the same facility shall be assigned logon IDs that are identical. Facilities where users have identical names shall add a numeric digit at the end of the logon ID to make it unique.

User Agreement

Designated Personnel. Users, including contractor personnel, designated by the Information Security Officer requiring access to the [ORGANIZATION] computers under the [ORGANIZATION] contracts must complete and sign a [ORGANIZATION] Request for Computer Access Form.

Computer Logon ID Password

A password is a unique string of characters that a user, programmer, or computer operator shall provide in conjunction with a logon ID to gain access to all of the [ORGANIZATION] computer system resources.

Password Standards

User Authentication

All systems shall require a valid user ID and password. All unnecessary operating systems or application user IDs not responsible and accountable to an assigned individual user shall be deleted or disabled.

Assignment of Passwords

The initial password issued by a security administrator must be valid only for the user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done. The minimum length of passwords shall be eight (8) characters. All users will automatically be forced to change their passwords at least once every thirty (30) days. All passwords must be promptly changed if they are suspected of being disclosed or have known to be disclosed to unauthorized parties. Passwords shall be maintained as sensitive information.

Any computer output that identifies a user's password shall be kept confidential to prevent unauthorized personnel from gaining knowledge of the password.

Forced Change of All Passwords

Whenever an unauthorized party has compromised a system, system managers shall immediately change every password on the involved system. Even suspicion of a compromise likewise requires that all passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded. Similarly, under either of these circumstances, all recent changes to user and system privileges must be reviewed for unauthorized modifications.

Password Storage

Passwords shall not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls.

Choosing Passwords

To obtain a new password, a user shall present suitable identification. All user-chosen passwords for computers and networks must strike a balance between difficult to guess and easily remembered. Difficult-to-guess passwords are those that contain at least one alphabetic and one nonalphabetic character. Words in a dictionary, proper names, geographical locations, common acronyms, slang, derivatives of User IDs, and common character sequences, such as "123456", must not be employed. Likewise, personal details, such as spouse's name, automobile license plate number, social security number, and birthday, must not be used. Enforcement password software should be used to either generate user passwords or validate the creation of a difficult-to-guess password.

Logon IDs

Sensitive user IDs, such as system administrators, power users, and information systems security professional shall have their passwords changed at least every thirty (30) days.

Previous Password History File

On all multi-user machines, system software or locally developed software must be used to maintain an encrypted history of previous passwords. This history file must be used to prevent users from reusing passwords. The history file must minimally contain the last thirteen (13) passwords for each user-ID.

Encryption of Passwords

To prevent passwords from being disclosed to sniffer attacks, passwords must always be encrypted when held in storage for any significant period of time or when transmitted over communications systems.

Prevention of Password Retrieval

Computer and communication systems must be designed, tested, and controlled so as to prevent the retrieval of stored passwords--whether they appear in encrypted or unencrypted form.

Reliance on Operating System User Authentication Process

Application systems developers must consistently rely on the password access controls provided by an operating system or an access control package that enhances the operating system. Developers must not construct separate mechanisms to collect passwords or user-IDs, nor must they rely on other mechanisms to identify or authenticate the identity of users.

Changing Vendor Default Passwords

All vendor-supplied default passwords must be changed before any computer or communications system is used.

Writing Passwords Down and Leaving Where Others Could Discover

Passwords must not be written down and left in a place where unauthorized persons might discover them. Users must not write their passwords down unless they have effectively concealed such passwords in a phone number or in other seemingly unrelated characters.

Password Sharing Prohibition

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms.

Password Constraints

The display and printing of passwords shall be masked, suppressed, or otherwise obscured so that unauthorized parties shall not be able to observe or subsequently recover them. Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.

Disclosure of Incorrect Login Information

When logging into a computer system or data communications system, if any part of the login sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the login process was incorrect after all of the login information has been entered. The number of consecutive attempts to enter an incorrect password shall be strictly limited to prevent password guessing attacks. After three unsuccessful attempts to enter a password, the involved user-ID shall be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than fifteen (15) minutes, or (c) if dial-up or other external network connections are involved be disconnected. This risk choice will depend on the sensitivity and criticality of the system being accessed.

Prohibition of Multiple Simultaneous On-line Sessions

Unless the system manager in writing has granted permission, no user is to conduct multiple simultaneous on-line sessions.

Automatic Log-Off Process

If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for five (5) minutes, the system must automatically either blank the screen or use a screen saver image, and suspend the session. Re-establishment of the session must take place only after the user has provided the proper password.

Computer Logon ID Suspensions and Cancellations

Inactivity

Any computer logon ID not utilized for ninety (90) days will be suspended, cancelled, or deleted. A user having a computer logon ID suspended must contact the System Administrator, Access Control Team, or the Information Security Representative at the affected facility to have the computer logon ID reinstated for use. A computer logon ID deleted because of inactivity will require that a new [ORGANIZATION] Request for Computer Access Form be submitted.

Misuse

The misuse or appearance of misuse of a computer logon ID and/or violations to computer security may result in disciplinary action, criminal prosecution, and suspension of the logon ID. Any detected misuse of a computer system will be reported to the Information Security Officer.

Termination or Reassignment of a Computer Logon ID

Termination

The manager of a user who is transferring (either within or out of the [ORGANIZATION]), retiring, receiving disciplinary action, etc., must request the deletion of the computer logon ID by completing and submitting a [ORGANIZATION] Request for Computer Access Form to the Access Control Team. The [ORGANIZATION] Request for Computer Access Form shall remain on file for two (2) years after termination of the logon ID. Logon IDs terminated should remain in an inactive state for a period of one (1) year before being reassigned. The Access Control Team will request a monthly list from Human Resource of all users that have terminated to ensure that the manager of a terminated user has submitted the Request for Computer Access Form.

Multiple User Logon IDs

1. A user may have multiple logon IDs documented by a single [ORGANIZATION] Request for Computer Access Form. Photocopies of the original form can be sent to other sites and Data Owners to obtain access. The photocopy must be signed by the user and the user's manager and must explicitly state the location of the original [ORGANIZATION] Request for Computer Access Form.
2. If multiple user logon IDs are used for remote system management or remote application support, only one of the [ORGANIZATION] Request for Computer Access Form is needed. This [ORGANIZATION] Request for Computer Access Form must be filed at the central site performing the remote system management or remote application support.

Each remote site does not need a copy of the original [ORGANIZATION] Request for Computer Access Form on file, but may receive one upon request.

Operating System Security Features

Processing Financial Information

Computer systems processing financial information shall be secured from unauthorized access. All security features shall be available and activated. Audit facilities are utilized to assure that everyone who accesses a computer system containing financial information is responsible and accountable. All programs, including third- party purchased software and applications developed internally by the [ORGANIZATION], shall be password protected. Computer logon ID passwords must be implemented where supported by operating system software. Passwords shall be stored in an encrypted format.

Browser Warning Logon Banner

An additional warning banner that states the user understands that the penalty for unauthorized browsing shall be placed on any of the [ORGANIZATION] computers that store Financial information so that the user must enter a keystroke to continue processing.

Financial Information Segregation

If financial information is recorded on removable storage devices or media with other data, it shall be protected as if it were entirely financial information. Only employees with “need-to-know access” shall be permitted access, and minimum safeguards will be implemented to limit unauthorized access to ensure confidentiality.

Emergency and Temporary Access

Emergency and temporary access authorization shall be controlled. Access control implementation includes a procedure for emergency access and, at least, one of the following features: (a) context-based access; (b) role-based access; and (c) user-based access. Emergency and temporary access authorizations are: (a) documented on standard forms and maintained on file; (b) approved by appropriate managers; (c) securely communicated to the security function; and (d) automatically terminated after a predetermined period.

Tokens

Users shall maintain possession of their individual tokens, key cards, etc., and understand that they do not loan or share these with others and that they are to report lost items immediately.

Clock Synchronization

All [ORGANIZATION] computers containing sensitive financial information or corporate financial data shall have their clock synchronized to a central timeserver to ensure accurate time on events being logged.

Remote Access

The number of users who can access into the system from remote locations shall be limited, and justification for such access has to be documented and approved by Data Owners. Managers and Data Owners must approve access to the [ORGANIZATION]’s computer resources from remote locations. If a remote access system utilizes dial-up modems, they must be expressly configured to provide secure network access. Access to the [ORGANIZATION]’s internal network from

outside of its defined network perimeter must be controlled by privileged access controls. When remotely accessing from a location not directly connected to the LAN, databases containing Financial information data shall adhere to the following: (a) authentication shall be provided through user ID and password encryption for use over public telephone lines; (b) authentication shall be controlled by centralized Key Management Centers/Security Management Centers with a backup at another location; (c) standard access shall be provided through local telephone numbers to local data facilities; and (d) access methods (local numbers) require a special encrypted modem for every applicable workstation and a smart card (microprocessor) for every remote user. Smart cards shall have both identification and authentications features and provide data encryption as well.

1. Logs of all inbound access into the [ORGANIZATION]'s internal network by systems outside of its defined network perimeter must be maintained. System administrators shall regularly review these logs or use automated intrusion detection systems to inform them of suspicious activity.
2. It is the responsibility of the [ORGANIZATION] employees with dial-in access privileges to ensure non-employees that they will not be granted dial-in access privileges to the [ORGANIZATION]'s information system resources, and that they will not be granted use of dial-in connections to the [ORGANIZATION]. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and the [ORGANIZATION] are literal extensions of the [ORGANIZATION]'s corporate network, and that they provide a potential path to the [ORGANIZATION]'s most sensitive information. The employee and/or authorized third-party individual must take every reasonable measure to protect the [ORGANIZATION]'s assets.
3. Analog and non-GSM digital cellular phones cannot be used to connect to the [ORGANIZATION]'s corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to the [ORGANIZATION]'s network.
4. Dial-in accounts are considered "as needed" accounts. Account activity is monitored, and if a dial-in account is not used for a period of six (6) months, the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

Data Files and Software Logical Control

Logical controls shall be implemented for data files and software programs regardless of their location within the IT infrastructure. Security software shall be used to restrict access. Access to security software shall be restricted to security administrators only. Security administration personnel shall set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files, and operating system files. Standardized naming conventions shall be used for resources.

Database and DBMS Logical Controls

Logical controls shall be implemented for databases and database management software (DBMS). Access to security profiles in the Data Dictionary and security tables in the DBMS shall be limited. Access and changes to DBMS software shall be controlled. Use of DBMS utilities shall be limited. DBMS and Data Dictionary controls shall be implemented in the following manner: (a) restrict access to data files at the logical data view, field and field-value level; (b) control access to the Data Dictionary using security profiles and passwords; (c) maintain audit trails that allow monitoring of changes to the Data Dictionary; and (d) provide inquiry and update capabilities from application program functions, interfacing DBMS, or data dictionary facilities.

Rationale

Networking is inevitably becoming more and more vital to the [ORGANIZATION]. The [ORGANIZATION]'s enterprise networks are not only communication media for employees, but they are transforming into a huge integrated information repositories of financial information and corporate financial data. Security aspects must be taken into account at an early stage when trying to establish advanced [ORGANIZATION] networking functionalities. The three basic dimensions of security - *information confidentiality, integrity and usability (accessibility)* - are in close relation with *access control*. This policy covers all individuals responsible and accountable for the protection of sensitive information computer and communication devices, owned or operated, by the [ORGANIZATION]. This policy assures financial that information is properly safeguarded and that the [ORGANIZATION] has the capability to deal with the growing threat of computer-based attacks in order to mitigate the risk of serious disruptions and damages to its critical infrastructure.

Risk

Failure to comply with this stated policy may place the [ORGANIZATION] in irreparable harm. Non-compliance with this policy and supporting policies pertinent to information security regarding computer crime is subject to management review and action in conformance with Agency disciplinary policies, State or Federal laws. If access control solutions capabilities are not provided, then the ability to analyze and trace the [ORGANIZATION]'s user actions will be severely limited and will not meet the legal requirements of both Federal and State laws. Failure to meet this security requirement could cause loss of the [ORGANIZATION]'s information sharing with business partners. If access control solutions are not implemented and configured properly, they can cause unauthorized browsing of financial information.

Impact

All areas of the [ORGANIZATION] shall comply with this identification and authentication policy; otherwise, an exception to the policy should be filed (and approved prior to implementation) if the policy requirement is not met.

Users

This policy shall impact all users who have access to the [ORGANIZATION]'s network or systems. This policy illustrates that any unauthorized access to the network or systems is

recorded, and that the [ORGANIZATION] holds the individual user accountable and responsible for unauthorized access.

Data Owners

This policy assists the data owners in assuring that only authorized users have access and that unauthorized access will be determined and prevented when possible.

Managers

This policy shall allow management to take appropriate action to ensure that all users are aware of the access and authorization control requirement for access to the [ORGANIZATION]'s information assets. This policy allows management to initiate or direct the development of a procedure for emergency access to information in the event of a crisis, and the unavailability of critical resources or assets to gain access to the information.

Application Development and Database Administrators

These administrators are responsible for implementing and monitoring approved access control solutions on the [ORGANIZATION]'s computer systems. It ensures that all sensitive applications have the appropriate audit functions to abide by Federal and State laws, and policies.

Access Control Team

The Access Control Team needs to ensure that continuity of access control solutions meet the needs of Application Owners/Data Owners. They also shall provide guidance or report to appropriate authorities vulnerabilities relating to the [ORGANIZATION]'s access control solutions.