

**National Association of REALTORS®
Center for REALTOR® Technology**

REALTOR® Secure Program

**REALTOR® Certified Online Presence
Evaluation Guide**

Version 1.27

November 18, 2003

Table of Contents

I.	Introduction.....	3
II.	Levels of Certifications	4
III.	National Association of REALTORS® Secure Goals	6
IV.	National Association of REALTORS® Security Standards.....	7
V.	Broker Evaluation Requirements.....	14
VI.	Evaluation Tasks and Report	15
VII.	Participation Tasks and Certification Process Flow	18
VIII.	Glossary	20



I. Introduction

The National Association of REALTORS® (NAR) has developed a security program to improve the overall security posture of its members and service providers. The program is based upon information security industry best practices.

Participation in the program can lead to your organization being certified by NAR, allowing your organization to be recognized as a security-aware organization by your customers, business partners and employees.

At the present time, there are three different types of certifications that can be obtained by various organizations:

- REALTOR® Certified Service Provider (RCSP)
- REALTOR® Certified Online Presence (RCOP)
- REALTOR® Certified Security Evaluator (RCSE)

If you are a Broker or Agent, this document contains information to be used as a guide through the various standards, processes, and guidelines, including:

- Learn about the various Levels of Certification
- Learn about the NAR Security Standards
- Learn about the tasks that will be performed to evaluate your organization
- Learn how to follow the proper evaluation process to become a REALTOR® Certified Online Presence
- Find a Evaluator from a list of REALTOR® Certified Security Evaluators
- Learn about the terms used through out the REALTOR® Security Program



II. Levels of Certifications

Participation in the program can lead to becoming certified by passing a defined security evaluation performed by a REALTOR® Certified Security Evaluator.

Participants in the program have been divided into three classifications, categorized by business role. Two of the classifications (Service Provider and Broker) are further divided by size. The classification and size differentiators play a strong role in the level and complexity of the participant evaluation requirements.

The three types of certifications that can be obtained by participants are:

Service Providers

Service Providers are defined as organizations providing online data services to a real estate brokerage or agent. For example: an online Multiple Listing Service for a particular area or an Application Service Provider (ASP) used to host an online presence for a brokerage or agent. Service Providers participate through the REALTOR® Certified Service Provider program.

Sizing for the REALTOR® Certified Service Provider program is defined by the number of agents serviced. These are broken down into small, medium, and large service providers and are defined as:

- Small – Less than 250 agents serviced
- Medium – 250 to 2000 agents serviced
- Large – Greater than 2,000 agents serviced

If the Service Provider is also an Evaluator, then they cannot self-evaluate.

Brokers or Agents

A Broker is defined as a real estate brokerage providing buyers and sellers an online service. For example, a broker in the town of Greenville, OH has an online presence containing listings of properties for sale in the area. A buyer or seller is able to view these listings and possibly contact the broker (or one of their agents) online through online forms, e-mail, live chat, etc. Brokers participate through the REALTOR® Certified Online Presence program.



Agents who operate an online presence separate from the Broker can apply for certification separately through the REALTOR® Certified Online Presence.

Sizing for the REALTOR® Certified Online Presence program is defined by the number of agents associated with a particular broker. These are broken down in to small, medium, and large brokers and are defined as:

- Small – Less than 25 agents
- Medium – 25 to 200 agents
- Large – Greater than 200 agents

Agents use the same program qualifications as Small Brokers.

Evaluators

- Evaluators are typically organizations with information security as their core competency, that have been certified by NAR as being able to accurately provide, with a high level of integrity, the security evaluation of both Service Providers and Brokers.



III. National Association of REALTORS® Secure Goals

The main goal of the REALTOR® Secure Program is to raise the security awareness of the real estate industry by supplying a set of standards and guidelines to follow. As a result of the adoption of such standards and guidelines an organization will be in the position to preserve the confidentiality, integrity and availability of real estate information.

Confidentiality

The practice of sharing information only with authorized individuals and organizations.

Integrity

The practice of maintaining information that is authentic and complete.

Availability

The practice of maintaining systems used for processing, delivering, and storing real estate information so they are accessible when needed.



IV. National Association of REALTORS® Security Standards

The REALTOR® Security Program uses the information security industry's best practices as its foundation. There are many international organizations, which have developed guidelines to help an organization increase their security posture. NAR has utilized three standards or security program models in the development of its security program. While the applicability of each model may not map completely to the real estate business, NAR has found that many of their components can be utilized to in the formation of a REALTOR® Security Program.

The security industry standards and program models researched during the development of the REALTOR® Security Program are:

(ISC)² Common Body of Knowledge

The Common Body of Knowledge [CBK] is a compilation and distillation of all security information collected internationally of relevance to Information Security [IS] professionals.

ISO/IEC 17799:2000

The ISO/IEC 17799 is the International Standard for Information Technology code of practice in Information Security. In 2000, the British Standard for Information Security (BS 7799) was adopted by ISO/IEC as ISO/IEC 17799.

VISA CISP “Digital Dozen”

The “Digital Dozen” is list of twelve basic security requirements with which all Visa payment system constituents need to comply.

The following lists of items contain the security standards that an organization should follow to participate in the REALTOR® Secure Program. These should be seen as the overall security standards recommended by NAR, but some may not apply to your organization, based upon its size. A REALTOR® Certified Security Evaluator will advise your organization on which standards are applicable. You should read and understand each of the standards and be prepared to discuss or ask questions about them with your Evaluator.

Security Policy

This refers to the documented policies that contain the fundamental principals and goals for maintaining a secure environment.



- A policy document should be approved by management and published and communicated, as appropriate, to all employees.
- The policy should state management commitment and set out the approach to managing information security.
- As a minimum, the following guidance should be included:
 - a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing
 - a statement of management intent, supporting the goals and principles of information security
 - a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, for example:
 - Compliance with legislative and contractual requirements
 - Security education requirements
 - Prevention and detection of viruses and other malicious software
 - Business continuity management;
 - Consequences of security policy violations;
 - A definition of general and specific responsibilities for information security management, including reporting security incidents
 - References to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with

Physical Security

This refers to method of protecting against unauthorized individuals gaining access to certain physical locations containing business critical components and data within the organization.

- The security perimeter should be clearly defined.
- The perimeter of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access, e.g. control mechanisms, bars, alarms, locks etc.
- A manned reception area or other means to control physical access to the site or building should be in place. Access to sites and buildings should be restricted to authorized personnel only.



- Visitors to secure areas should be supervised or cleared and their date and time of entry and departure recorded. They should only be granted access for specific authorized purposes.
- Access to sensitive information and information processing facilities, should be controlled and restricted to authorized persons only. Authentication controls, e.g. swipe card plus PIN, should be used to authorize and validate all access. An audit trail of all access should be securely maintained.
- All personnel should be required to wear some form of visible identification and should be encouraged to challenge unescorted strangers and anyone not wearing visible identification.
- Access rights to secure areas should be regularly reviewed and updated.

Remote Access

This refers to ability for users or systems to access internal resources and information from a location outside of the physical corporate office or campus.

- Only users with a specific business requirement should be granted remote access to corporate network resources.
- User should be authenticated at the time of connection by the remote access gateway prior to being granted access to corporate network resources.
 - At a minimum authentication of remote access user should be in the form of a unique user name and password and follow the recommended password choice guidelines (see User Management).
 - Two-factor authentication can be used to mitigate the threat of passwords being guessed or shared by the organizations employees (e.g. RADIUS or TACACS with tokens).
- Whenever corporate data is transmitted over public networks in conjunction with a remote access solution, encryption should be used (see Data Encryption).

Network Access Control

The ability to designate which devices within the organizations network can communicate with other internal or external devices.

- Establish a formal process for approving all external network connections (e.g. Internet, 3rd Party, or Other).
- An access control device such as a firewall should be used to separate Internet and 3rd party (business partner) networks from the organization's internal network.
- Users should be placed on separate network segments from those of the server population. This must be separated by a firewall or equivalent access control devices.



- All access control policy should be created to disallow all access through the firewall by default. Specific policy rules must be created to allow access and documented for business purpose and usage such as:
 - Outbound Internet access (e.g. HTTP, HTTPS, FTP, POP3)
 - Inbound web protocols (e.g. HTTP, HTTPS)
 - System administration protocols (e.g. SSH, SCP)
 - Other protocols required by the organization
- Implement network address masquerading to prevent internal addresses from being translated and revealed on public networks.
- All access control policies should be audited by internal staff on a quarterly basis to identify out dated policy rules.

Intrusion Detection

This refers to ability for an organization to detect malicious activity on their systems and networks.

- An intrusion detection device should be installed and configured to examine network traffic at locations where access control devices separate organization, 3rd party and public networks.
- The intrusion detection device should be configured to alert security personnel via manageable means in the event that unauthorized access is detected.
- The intrusion device's software and attack signatures should be updated on a regular basis.
- At an organization where 24/7 monitoring of the device is not feasible, the organization should consider outsourcing the monitoring responsibility to a trusted 3rd party.

Virus Protection

The methods that the organization uses to maintain the software run on systems is safe and free of malicious code (i.e., viruses).

- Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Protection against malicious software should be based on security awareness, appropriate system access and change management controls.
- The following controls should be implemented:
 - Install and regularly update of anti-virus detection and repair software to scan all computers and media on a routine basis.
 - Conduct regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated.



- Check all files on electronic media of uncertain or unauthorized origin, or files received over untrusted networks, for viruses before use.
- Check all electronic mail attachments and downloads for malicious software before use. This check should be carried out at different places, e.g. at electronic mail servers and desk top computers.

System Security

This refers to ability to maintain secure servers and workstations within an organization's environment.

- Always change the vendor-supplied defaults before a system is placed into production.
- Maintain a company standard system build for each device class in the environment. The build should take into account all known security vulnerabilities and industry best practices related to the system.
- Implement only one application or primary function per server (i.e. run the mail server on a different physical computer from the web server).
- All systems should be configured to only run necessary services.
- All systems and software should be kept up to date with the latest vendor supplied security patches.
- Install new/modified security patches within one month of release.
- Test all security patches before they are deployed to production systems.
- Implement and follow change control procedures for system software configuration.
- Implement a process to identify newly discovered security vulnerabilities.

User Management

This refers to ability to delegate authorization by individual in the access of systems and applications.

- Uniquely identify all users before allowing them to access system and network resources.
- Use at least one of the methods below to authenticate all internal and external users:
 - Unique username and password
 - 2-factor (e.g. tokens or certificates)
 - Biometrics
- Ensure proper password management by:
 - Controlling the addition, deletion, and modification of user IDs.
 - Immediately revoke access of terminated employees
 - Distributing password policies, procedures and guidelines to all users on a regular basis
 - Not permitting group passwords



- Changing user passwords every 90 days.
- Requiring a minimum password length of at least 7 characters.
- Should not be found in a dictionary of commonly used words.
- Using passwords that contain both at least 1 number and 1 symbol (e.g. !, @, #, or %)
- Monitoring access attempts.
- Locking out users after 6 failed authentication attempts.

Data Encryption

This refers methods of storing and transmitting data using cryptographic technology to maintain confidentiality and integrity.

- Implement a cryptographic solution that:
 - Is isolated so that secret data cannot be disclosed
 - Conforms to applicable international and national standards
- Protect encryption keys against both disclosure and misuse by:
 - Restricting access to the encryption key to the fewest number of individuals
 - Store encryption keys securely in the fewest possible locations
- Fully document all key management processes and procedures.
- All organization originated data that is transmitted over public networks should be encrypted so that it can only be decrypted by its intended recipient (e.g. SSL and IPSec).
- Data classified as business confidential that is transmitted over organization networks, should be encrypted so that is can only be decrypted by its intended recipient.
- Data classified as business confidential should always be stored (when possible) in an encrypted form, so that it can only be accessed by systems or individuals specifically requiring such access.

Disaster Recovery

The organization's documented process for ensuring the acceptable availability of their environment for the online services they are providing.

- Backups of systems containing business critical data (i.e. financial data, employee records, client records) should be made on a daily basis.
- At least one back up per week should be should be stored at an offsite data storage facility.
- Restoring systems and data from backups should be tested on a regular basis.
- All systems or data connections providing critical business functions should be made highly available, e.g. application and database servers, data carriers, firewalls and authentication systems





V. Broker Evaluation Requirements

In the table below, various Broker sizes have been mapped to an evaluation requirement. Also, the estimated effort by your Evaluator and cost to your organization has been identified. These estimated costs are for security assessment only and do not include remediation services.

Exhibit 1: REALTOR® Security Program – Broker Evaluation Requirements

Certification	Size	Evaluation Requirement	Estimated Effort	Estimated Cost to Broker
REALTOR® Certified Online Presence	Small	Questionnaire Phone Checklist Remote Scan	3 – 10 hours	\$500.00 – 2,000.00
	Medium	Questionnaire Phone Checklist Remote Scan Documentation Review	12 – 20 hours	\$2,000.00 – 4,000.00
	Large	Questionnaire Face-to-Face Interviews Remote Scan Documentation Review	36 – 60 hours	\$5,000.00 – 10,000.00



VI. Evaluation Tasks and Report

There are 5 different possible tasks that your Evaluator can perform during the evaluation. Based upon the size of your organization, there may be some items outlined below that are not performed. The possible tasks include:

Questionnaire – The questionnaire has been developed to serve as a pre-evaluation data gathering tools. It will be provided to you by your Evaluator or it can be downloaded from NAR. The information requested ranges from general contact information to information about your network environment. It is important to answer each of the questions with the most accurate and detailed information you can provide.

Checklist – A security checklist has been developed for the REALTOR® Security Program. The checklist covers questions pertaining to each of the REALTOR® Security Standards. Your Evaluator will walk you and possibly other members of your organization through each of the questions. All of the answers to the questions will be either “Yes” or “No” with some explanation about how the standard is or isn’t followed in your organization. To prepare for the checklist, you should review each of the security standards outlined in this document. Think about how your organization meets each of the standards. If you don’t know about the area some of the standards represent, you should refer your Evaluator to someone in your organization that has more experience in that particular area than you do. It is important to provide your Evaluator the most accurate answers as possible.

Face-to-Face Interviews

An interview consisting of a walk through of the above checklist may take place depending on the size of your organization. These interviews will be limited to 4 individuals within your organization. Each separate interview will be limited to 1 hour.

Individuals requiring separate face-to-face interview can include:

- IT Director
- Security Manager
- Network Administrator
- System Administrator
- Database Administrator
- Application Developer

Remote Security Scans



Your organization is required to undergo a Remote Scan of their environment as part of the evaluation. A remote scan will utilize open source tools to evaluate network and system configurations as seen from the Internet. In addition, the tools will be used to identify any vulnerability present within network and system devices. No Denial of Service (DoS) scans will be run by your Evaluator. Your organization is required to undergo a Remote Scan of their environment as part of the evaluation.

Documentation Review

Your Evaluator will gather documented diagrams depicting the configuration and organization of device on your network. Your Evaluator will examine these diagrams for security industry best practices and make recommendations for improvement. You should try to gather these documents prior to the evaluation. At your Evaluator's request, you can provide the diagrams to them prior to the start of the evaluation.

Report Guidelines

It may take about week (after the conclusion of the evaluation) for your Evaluator to develop the report. After the report is developed a draft copy for your organization for review before it is sent to NAR.

The report will contain the following information:

- Executive Summary
 - Include the following:
 - The nature of the Broker's business.
 - The Broker classification (i.e. Medium Broker)
 - A description of the environment in which the evaluation was focused (i.e. the organization's Internet access points, internal network)
 - A statement stating recommendation for or against certification:
 - Yes
 - Yes, after some changes (changes listed)
 - No
- Scope of Work and Approach
 - A description of the depth to which the evaluation was performed and a high-level overview of the methodology
 - Timeframe of the evaluation (i.e. when where the tasks performed?)
- Findings and Observations



- The document results of each of the evaluation tasks performed
- Recommendations for remediation of any non-compliant items
- Contact Information and Report Date
 - Broker Contact Information
 - Evaluator Contact Information



VII. Participation Tasks and Certification Process Flow

You should begin by review the security standards outlined in this document. Once you are familiar with each of the security standards, you should perform a self-assessment by comparing each of the REALTOR® Security Program Standards to your organization's environment.

You should then remedy any discovered shortcomings by utilizing internal staff or by contracting an outside information security firm for assistance. You should also work to communicate importance of the REALTOR® Security Program within your organization.

When making changes to your environment, refer to the REALTOR® Security Program Standard to ensure decisions are following information security best practices.

Your organization can become REALTOR® Certified by undergoing a security evaluation by a REALTOR® Certified Security Evaluator once every 2 years.

Exhibit 2: REALTOR® Security Program Evaluation Process Flow

1. You should locate a REALTOR® Certified Security Evaluator listed in this document and contact them. Tell them you would like to begin a REALTOR® evaluation.
2. Discuss your organization's evaluations requirements with the Evaluator.



3. You will be provided with a Statement of Work (SOW) by the Evaluator with the description the evaluation tasks to be performed and the estimated costs. You should ask the Evaluator for an explanation of each of the items and costs outlined.
4. Your organization signs-off on the SOW and submits to your Evaluator the appropriate payment arrangement.
5. Your organization participates in the evaluation providing your Evaluator with all information requested.
6. One week after the evaluation, your organization will receive a draft report from your Evaluator. You have one week to review the draft and respond to any of the findings to your Evaluator.
7. After your comments have been received by your Evaluator, you will receive a final report.
8. Your Evaluator will deliver the final report to NAR. You should then wait for NAR to respond with certification results.
9. If the results of the certification are positive, then you will receive a certification package from NAR. Else, your organization should perform remediation based upon the recommendations provided in the final report. When the environment is ready, your organization should participate in a re-evaluation of the environment.



VIII. Glossary

Attack Signatures – The network traffic patterns used by IDS (see Intrusion Detection Systems) to detect a potential hacking attempt.

Audit Trail – The chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

Biometrics -- A method of generating authentication information for a person by digitizing measurements of a physical characteristic, such as a fingerprint, a hand shape, a retina pattern, a speech pattern (voiceprint), or handwriting.

Business Continuity Management – The combined emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis.

Certificate – A digital data document assigned to object (system or individual) used to authenticate the object during a transaction (system or network access, data exchange, etc.)

DNS – An acronym for Domain Name System. The main Internet operations database, which is distributed over a collection of servers and used by client software for purposes such as translating a domain name-style host name into an IP address (e.g., "www.realtor.org" is "32.97.215.193") and locating a host that accepts mail for some mailbox address.

Encryption Key -- A cryptographic key that is used to encipher application data.

Firewall -- An internet-work gateway that restricts data communication traffic to and from one of the connected networks and thus protects that network's system resources against threats from the other network.

High Availability -- The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.



Information Security Industry Best Practices – a collection of internationally accepted processes and technologies used by organizations to secure data processing environments.

Intrusion Detection System – A security service that monitors and analyzes system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Malicious Activity – An action performed by an individual, virus or worm intentionally harming a system, network, application or data.

Network Address Masquerading – A network where packets traveling to and from the internal network are translated for private addresses, so they are not revealed to the public.

Remote Access Gateway – A device that user or devices dial into using a modem in order to gain access to resources on the network the device is attached.

Secure Areas – A location in a building where only authorized individual should be allowed to enter.

Security Patches – A code update intended to resolve a security issues within one or more of the components an operating system or software package.

Security Posture – The overall view of an organization from a security stand point.

Tokens – A device used by an authentication system to supply one time unique passwords.

Two-factor Authentication – A higher level of authentication than a unique user name and password. Something that a user has (a certificate or token) above something that the user knows (a password) make up the second factor of authentication.

Acknowledgments

Portions of the Glossary of Terms were obtained from IETF RFC2828
<<http://www.ietf.org/rfc/rfc2828.txt>>

