


# The Home Security Methodology 1.2



## VACATION GUIDE

## A Note to Vacationers

So you are going on vacation? Keeping closely to the ISECOM mission of “Making Sense of Security” we release the first ever ISECOM security Vacationing Guide for you! It is based on the ISECOM Home Security Methodology and focused on the best and most thorough way to secure your home for while you are away and making sure you stay safe on your trip. This guide aims to be the most thorough checklist available on this topic and we hope it makes you a safer and happier traveler!

This guide is open to assure that anyone can assist in making it the best possible home security vacation guide that it can be. An open methodology has the major benefit of a large and diverse number of reviewers and feedback. This also means that there is no cost or license for applying this methodology, sharing it, or integrating it into other works as long as you follow the requirements of the Open Methodology License available at the end of this manual and at [www.isecom.org/oml](http://www.isecom.org/oml).



This methodology follows the methodology of the OSSTMM (Open Source Security Testing Methodology Manual) a professional guide for a thorough security test. The OSSTMM is used around the world as the standard for security tests whether of computers, telephone networks, satellite relays, office buildings, or military bases. Since it has been designed to do the most thorough security test possible, fine-tuned through thousands of reviewers and practitioners, it had the most complete guideline on security and safety to apply to protecting one's home. The following concepts from the OSSTMM have been integrated to create this methodology:

<b>SECURITY</b>	<b>visibility</b> <b>trust</b> <b>access</b>
<b>SAFETY (Class A - interactive controls)</b>	<b>authentication</b> <b>indemnification</b> <b>subjugation</b> <b>continuity</b> <b>resilience</b>
<b>SAFETY (Class B - process controls)</b>	<b>non-repudiation</b> <b>confidentiality</b> <b>privacy</b> <b>integrity</b> <b>alarm</b>

## Version Information

The current version is HSM.VG 1.2. This current version is published on Thursday, July 17, 2008.

## Restrictions

This research document is free to read, apply and distribute under the Creative Commons 2.5 Attribution-NonCommercial-NoDerivs license.

As a collaborative, open project, this guide is not to be distributed by any means for which there is commercial gain either by itself or as part of a collection. As a standard, there may be only one, official version of this methodology at any time and that version is not to be altered or forked in any way which will cause confusion as to the purpose of the original methodology. Therefore no derivation of this methodology is allowed.

As a methodology it is protected under the Open Methodology License 3.0 which applies the protection as that granted to Trade Secrets however where a Trade Secret requires sufficient effort to remain a secret the OML requires the user make sufficient effort to be as transparent as possible about its application. Use and application of this methodology is acceptance of the responsibility of the user to meet the requirements in the OML. There are no commercial restrictions on the use or application of this methodology. The OML is available at the end of this manual and at <http://www.isecom.org/oml/>.

Any and all licensing questions or requests can go through ISECOM: [info@isecom.org](mailto:info@isecom.org).

## About ISECOM

ISECOM, the Institute for Security and Open Methodologies, is a registered Non-Profit Organization in Catalonia, Spain with an office in New York, USA, and Affiliates, Training Partners, and Licensed Security Auditors around the world. Financing for all ISECOM projects has been provided independent of commercial and governmental influence through ISECOM partnerships, subscriptions, certifications, licensing, and case-study-based research.

Your evaluation of this document, suggestions for improvements, and results of its application for further study are required for further development. Contact us at [info@isecom.org](mailto:info@isecom.org) or visit us at [www.isecom.org](http://www.isecom.org) to offer research support, review, and editing assistance.

## How to use this guide

Homes are both an asset and a form of protection for our assets. They are unique in that they have both a real and a personal (nostalgic) value. Securing our homes and making them safe for the ones we share it with is often more difficult than it should be. We want to live in a secure home but we don't want to feel like we live in a prison. **But then we go on vacation!** We want to make sure that our house can be converted into a fortress for our belongings, a safe haven for any family members staying behind, and a refuge for us to return to. To do this, we need to know security and of all the things we can secure about our home. This guide aims to be that course of action.

The guide follows the HSM methodology. In that methodology, you learn that security, the means of separating threats from assets, is the best way to avoid an attack. Then should an attack occur anyway, we cover the controls which you can have in place to thwart the threat or minimize damages. Therefore this guide will have you securing home before you are expected to find ways of controlling various, common threats. The concepts may seem as odd to you as a practice for protecting your assets. Part of the problem is that much of the existing security concepts are built upon old research. Some of these concepts you know about security may no longer be true if they had ever been true. Some current practices evolved from faulty logic, faulty or improperly conducted statistical surveys, urban folklore, and old, regional, or knee-jerk legislation.

If you are interested in getting more help with this or want to support this project, you can visit us at our website <http://www.isecom.org>. The OSSTMM Professional Security Analyst ([www.opsa.org](http://www.opsa.org)), OSSTMM Professional Security Tester ([www.opst.org](http://www.opst.org)), and OSSTMM Professional Security Expert ([www.opse.org](http://www.opse.org)) trainings will teach you how to think and act within the terms of this guide to quickly size up security, apply protection techniques, test those techniques, and measure the protection level for ANYTHING. This guide is an example of how that training can be applied.

## About Security and Safety

It is not the goal of the HMS to scare you. Life can be complicated enough without needing to paralyze you with fear from making bad choices. It is better to teach you how to make better choices than to risk scaring you into making none or poor ones.

The typical method of selling security and safety measures can be found everywhere from the government to the classroom. That method is to use FEAR, UNCERTAINTY, and DOUBT to accept someone else's idea of security. While this method may make for great marketing pitches it's not something that should be used to convince people as it will make them disregard it over time. Most people have been exposed to fear methods since they were able to watch television at the very least and with that constant exposure they develop a numbness towards it. Therefore marketers have had to get ever more drastic and prey on ever more intimate issues that will better sell their security products through fear. Don't believe them. Often times if you break down the statistics they throw at you, there is no information about the data pool or the definitions they are using. General statistics are used to sell you something by scaring you. For example, if you are told there is a robbery in America every 49 seconds (a common statistic), you need to understand:

1. Where did the data for this statistic come from? What year? What is the trend? Is it just a speculation from the author? How many people were asked? How many records were looked at? Were the records made and maintained by a competent source? How neutral was the statistic maker (was it paid for by a company trying to sell you something)?
2. How do they define a robbery? Do they count thefts worth under \$10US too or apparent break-ins where the home owner could not determine if anything at all has been stolen? Do they count thefts where the people were invited in, like at a party, where they proceeded to steal things semi-anonymously which is actually not the legal definition of a robbery.
3. Do they count reported robberies or confirmed ones such as when police investigations have concluded that a robbery occurred?
4. How was the 49 seconds time factor determined? We really can't believe that a robbery is made (or reported) every 49 seconds. They may get 10,000 reports across the nation all at once and then not again for a few hours.
5. Do they combine data sets of higher risk areas or large cities that may have 1000 robberies a night with lower risk rural areas like farms that have 1 robbery a year? Really though it matters because the statistic assumes we are all in the same place which is just another way to try to scare you.
6. Is that 49 seconds a mean number based on the whole data set of daily robberies and there are truly around 641,829 robberies (another perspective may be that it is about 1 for every 450 people) per year in America?

Keep in mind that statistics and generalizations are used to make you aware of something but you need to decide if it actually pertains to you, your lifestyle, and your needs. It's better to rationally dissect a general statistic first and accept the fact that it could be an attention-getter and may not even be a real problem for you. Then if there is something you want to change in your life because of it, consider logically all the solutions that really fit to the problem and not just the proposed solution in the advertisement or article (note that often newspapers and magazines are mostly paid by advertisers who may submit articles featuring their products or retain a journalist for public relations work).

## **What can happen to your home while you travel?**

At some point you will need to consider the bad things which can happen to your home or even the assets within while you are away. In this case, assets may even be family members not traveling with you. This means you should take some time to consider risks based on what you know are around you.

**Bad things are anything that can take, change, destroy, or hide assets, which in this case refers to the house, the people inside the house, and the things of real or sentimental value inside. In the study of Risk, a Threat is the “bad thing”. It is part of the basic equation where Risk = Threat x Asset x Vulnerability. Then the higher the number, the greater the risk.**

Therefore a threat only has power if you are vulnerable to it or you have something that it wants (assets). An asset is only at risk if there exists a threat. And a vulnerability only matters if you have something to be vulnerable to. But this guide will not address risk since it is a concept that is biased because it is so different depending on the person, the region, the environment, the law, and many other factors which cannot be possibly all covered here. Therefore we will only address operational security (OPSEC) and operational safety (OPSAF) as it applies to common threats and vulnerabilities.

Some common threats you might already know or need to understand:

- An intruder entering your home with the intention of theft, violence, destruction, or privacy violation.
- A trespasser hiding within your home or property.
- A stalker or voyeur outside your home looking in.
- A vandal outside your home destroying your property.
- Damages from wild animals, insect swarms or infestations, aggressive plants/weeds, allergens, and ground, air, or water contaminants like viruses, bacteria, radioactive materials, poisons, and organics (oil, body wastes, and plant and animal decomposition).
- Environmental damage from fire, heat, cold, ice, wind, electrical storms, flooding, or mud slides.
- Damages from power outages, power spikes, water shortages, sewage back-up, or lack of garbage removal.

## Security

When an asset is physically separated from a threat it is **secure** from that threat. Security will exist when 1) the assets are physically away from the threat or, 2) when the threat is eliminated or destroyed.

## Visibility

Opportunity is created by what can be seen or known of your assets. This is known as visibility. It is a two-sided coin. Visibility provides both a revealing of what you have (exposure) which may bring unwanted attention and for having safe approach and access to your home where an attacker may hide.

	TASK	COMPLETED
1	Make sure that neighbors can see your house if they need to. That means yard and porch lights on at dark and trim any shrubs or bushes that might overly obscure the entrance view from the street, trusted neighbors, security patrols, or police. For example, using light bulbs that turn on automatically when it's dark automatically.	
2	Stop deliveries. You want the house to look trafficked. Cancel papers, hold mail, and make sure no packages, milk, groceries or other deliveries stay on your doorstep.	
3	Keep your car in the garage if you have one or in the driveway if you don't. No need to keep another asset easily accessible if you don't have to. If your house is targeted then it is being watched and they will know that you are not home. If it's the case of a random burglary, they might take the car if no other security or control prevents them from doing it. A tight C-clamp on the track above the wheels of a garage door will keep it from opening even if unlocked.	
4	Keep your shades down about a week before you go so it looks normal. Most people do that anyway in summer to keep the house cooler. Then when you go, it won't look so odd if your house is being watched. Put plants that need a lot of light in the back yard or in the shower if your bathroom has a window. They sell opaque, static covers for bathroom windows you just cut out and stick on the glass. Then light can get in but people can't see in. They also sell automated watering kits if you don't have someone to water them. Don't forget to block door slots for mail, dog/cat doors, and vents from the inside to even prevent just peeking.	
5	Wherever you don't have shades, like doors with little windows, make sure that you can't see any of the "good stuff" while peeking in there. Anywhere that someone can peek into your house, regardless of the floor (people can climb) make sure the asset is out of view. That includes electronics, valuable collections, money, and your subscriptions to Forbes and Yachting magazine (ha ha?). If you have a safe, make sure it's out of sight and bolted into concrete. Thieves can and will take it with them otherwise. If you don't have one and want to buy one, get one from a hardware store far away, pay cash,	

	carry it out yourself, and install it yourself. If there are potential thieves working there then they shouldn't have your address. If you are really paranoid you could rent a van to pick it up so they don't get your plate numbers. Remember that every person you involve in the process makes more people who know you have a safe.	
6	Set your answering machine or voice mail to pick up immediately so it seems you may be on the phone when they called. You can even change the message to: "I'm on the other line right now, please leave a message and I will call you back." And leave away any automated e-mail responders that say you're on vacation at home and the office. If you must, just tell them you're unavailable but without the date range along with who they should contact in an emergency.	
7	Unless you have a house-sitter or babysitter, turn off the volume on your answering machine and telephones to reduce listening for ringing from outside the house as used in a common call-check to see if someone is home.	
8	If you are attending a funeral, wedding, wake or anything that's been announced in the newspaper or on-line, plan to leave a house-sitter and make your neighbors aware of the increased risk. Thieves read the paper too.	
9	Do not use automated lights. Even the random ones won't fool a thief unless they are also too deaf to hear footsteps and too blind to notice a lack of shadow movement in the house. Keep your house dark and a little safer from unattended electrical fires.	

## Trust

In security, when one target can interact with another target in the same scope, this is called a *trust*. In this case, those who you know from around the house, may still have access even though you are no longer there. People who you trust as long as you are around may not be someone you trust when you are away.

	TASK	COMPLETED
10	Let trusted neighbors know you're leaving and for how long. Ask if they will make sure no papers or packages stay on your doorstep. Have them check for and clean up any vandalism on the house-- and now is not the time to save money, offer to pay them! Depending on the level of trust, they may need a key in case of an emergency or know where to get one. But really, you're better off minimizing who can go in or near your house.	
11	If you're paying for a security service, don't tell them you're gone. Their job is to secure the place whether you're there or not and you don't want them treating the house any different then if they assumed you were around. Don't think because you're a customer that you have paid for trust. Their guards are just people with a job and you probably don't really know them.	
12	Hold your gardener, mowing service, paper delivery, postal delivery, and any other service that allows others to have access to your property. Minimizing interaction is key. This includes leaving pets with friends, neighbors, or animal hotels if possible or using automated feeders. But if you will be gone more than	



	2 weeks, do hire a mowing service to come weekly and tell them to go to your friend/neighbor for access to the property. This way someone trusted will know when they came and when they left, especially if an alarm needs to be deactivated and activated again.	
13	Ask a close friend or relative to come by the house occasionally to make sure everything is fine. This may be something you need to do if they have to come to feed your pets, walk your dog, etc. But do limit the keys you give out to your place. It leaves an opportunity for them to forget to lock the door or set the alarm when they leave. Remember to let the trusted neighbor know who will be checking the house, so that they do not call the police on them.	

## Access

Security is about preventing interaction. Access is direct interaction. There really are only two ways to steal something: 1) take it, or 2) convince someone else to take it and give it to you. Both means require interaction.

	TASK	COMPLETED
14	When you leave, close your shutters. Lock your windows. Bolt your doors. Use a pin, screw, nail, or bar to make sure they, especially large sliding doors, cannot be opened from the outside. I know it's against conventional wisdom to make your house look abandoned but looks aren't your worry. Thieves are. And preventing access is your first defense.	
15	Close all gates around the house and lock them. Lock tool sheds, yard boxes, etc. because you don't want to make it easy for a thief to get tools they need to open your locked doors and windows.	
16	For the car(s) staying at home, lock it, the glove compartment, and any part of it that can be locked.	
17	Lock any doors, cabinets, safe boxes, and desk drawers inside the house that can be locked with a key. While most of those locks can be picked or broken fairly easily, it costs the thief their time and sometimes their silence.	
18	Trim the tree branches which you can that hit your house when windy, conceal the views of any doors or windows, or provide access to windows.	
19	Close any gaps or rotted wood between door frames and window frames that will allow for tools to slip through or a frame to be pushed wider so the door or window pops out or off track. You can use your elite carpentry or welding skills to tighten them up from the inside or you could buy a can of foam that you can spray into the crack and will turn rock hard in a few days.	
20	Any outside hinges or bolts that have been screwed into the door with the screws outside of the house can be better protected with a few drops of solder on them.	

## Safety (Interactive)

When a threat or its effects are controlled then those assets are said to be safe. Safety will exist when the threat is limited in its ability to steal, hide, harm, disrupt, or destroy.

Interactive safety controls protect wherever the threat needs to interact within the target to be effective.

## Authentication

To give authentication is to provide someone with the right key and permission to access. Then when they gain access they have done so legitimately and by causing no damage.

	TASK	COMPLETED
21	Don't leave your hidden, emergency key in its usual place. Actually, don't leave it around at all. Put it inside in a safe hiding place or lend it to your trusted caretaker. Put away all your keys, for your car, spare house keys, boat, that little firebox under your bed, safety deposit box, and your garage, gate, and alarm remote controls, in an obscure hiding place. Don't forget that any passwords, PIN, codes, intimate photos or lifestyle details, check books, or credit cards should also be put away out of view and from being easily found.	
22	Shutdown your WiFi. Shut down or lock down your network ADSL/Cable router if you can (some people like to have remote access to home systems). If you need Internet access to your home, then make sure you set it up with a VPN, SSH, or some other means on non-standard port numbers. Experts will tell you that security through obscurity is not security. Those experts are wrong. Do it because the lowest common denominators like worms and zombie boxes look almost always for default ports and then move on.	
23	Change your alarm code and only tell those you trust to watch the house this time.	
24	Change the combination on your safe.	
25	Get a passive infra-red alarm system for your house and yard. Even the wireless ones are good if they offer tamper and jamming protection. No outside access point (window, door, crawl space) should be accessible without being in range of the sensor. No sensor should be in a location where a person can get behind it and blind it with glass or an opaque sticker without being in the view of another sensor. Reduce false alarms by assuring the sensors don't point at limbs of trees or water which can reflect the infrared energy and create false positives when the wind blows. Make sure every room with assets, especially the one with the safe, has a sensor opposite the entry point. Put a sensor in your garage and basement too. Don't forget to protect the porch and roof by assuring anyone trying to climb up would be in sensor view. Most of the alarm systems can be installed easily by you. Many come with software to hook them up to your computer for easy configuration. Buy a system that will have the ability to call you by phone and should that fail, by mobile. Then make sure it can call you immediately whenever it goes off. The siren itself should be in a discrete place at the front of your house and you should talk to your neighbors about the sound so they recognize it. However	

	do not depend on them to investigate. So if you want to spend extra on having a service where a guard gets sent out when the alarm sounds, that's okay but not necessary if you live where you have close friends who live near by that can investigate while you are away.	
26	Change your fire alarm or flood alarm batteries. If you can, get ones that hook into your security system so it also calls you.	
27	Let all care-takers, house-sitters, or baby-sitters meet so they can know about each other.	

## Indemnification

To add indemnification as a control you are making clear the rules for interactions or actions with a clear warning message, insurances, and the use of legal protection services like policemen, security guards, and prosecutors to act upon those warnings.

	TASK	COMPLETED
28	Put a sticker on your door or mailbox that you want no solicitors or junk mail even if it's just while you are gone.	
29	If you have an alarm, dog, or a surveillance service then keep it discreet and leave the alarm or warning sign away. Professional thieves don't care about them and you take away the element of surprise (unless it's the bad for you kind of "Hey, surprise, we have a fake sign and no dog or alarm!" as they proceed to break in). Signs only inform a thief to be more cautious.	
30	If you have a large property, post clear warning signs around it that it is private property and no trespassing is allowed.	
31	Make sure your name and Driver's License number are etched or engraved into all your assets where possible, like cameras, computers, televisions, stereos, bicycles, and anything else of value which could find its way to a pawn shop.	
32	Get insured. It will require you to inventory and take pictures or video of all your assets as well as all the rooms of the house from various angles to be sure to include everything- even your furnace. Keep a list of serial numbers for all the costly or difficult-to-replace items as well. Make sure you insure yourself for the environmental dangers in your region as well as theft. Getting an independent audit for following a thorough security methodology like the HMS from ISECOM will get you a discount from some insurers.	

## Subjugation

This control assures that security decisions come from you and you leave no choice for others on how to follow that decision. For example, a door that locks only on the inside does not give the person outside a choice to use a key or pick the lock.

	TASK	COMPLETED
33	Make sure all doors and windows with bolts and locks can only be opened from the inside except the main door where you will need to enter upon your return. Even outdoor power outlets should be locked with special locks that can be plugged in and opened with a key.	
34	Tell your bank to note the dates of your travel and set hard limits on your credit cards and ATM. Tell them if you will not be writing any checks. If you're at a small-town or familiar branch and can ask them to let you sign off on a code word so that if you need to change it by a phone call, they will accept that code as a signature.	
35	Be sure the house-sitter and babysitter know that only they are to answer the door or the phone and should screen all persons first either through a peep hole or an answering machine. Trusted people will know they are being screened and will announce themselves then wait for the caretaker to respond.	

## Continuity

When you want to make sure things keep going as they should you provide controls of continuity.

	TASK	COMPLETED
36	If you have bug, pest, or rodent infestation problems, time the exterminator to come just before you leave. Otherwise set up traps and repellent in key OUTSIDE areas because if you're gone more than a week you may come home to nasty, rotting stuff.	
37	Clean out your fridge of any spoilables and make sure your freezer is on a medium setting which should be acceptable since nobody will be opening it if nobody is home. If your refrigerator has a water tray underneath it, be sure it's empty.	
38	Be sure not to leave any fruit, bread, or other spoilables out or around. Be sure the sink is clean of dirty dishes and standing water.	
39	Drain any stagnant or standing bodies of water around the yard which could collect fly larvae in. Over-turn anything that will collect water should it rain while you are gone. While you're at it, remember to bring inside anything that should not get too much sun (some things fade in the sun) or get too wet.	
40	Back-up important data, photos, and home videos onto an external hard drive and put it in a safe, at a trusted person's home, or in a safe deposit box.	
41	Write down or photocopy all your credit card and emergency contact	

	information as well as important telephone numbers for those cards and your bank in case your wallet gets stolen. Make a copy and give it to a very highly trusted person. You do not need to know your whole credit card number to cancel it so only write down the last 5 digits and expiration date.	
42	Minimize what papers and documents you will take with you to only what is necessary. It's a good time to clean out your wallet, purse, backpack, briefcase, computer bag, or glove compartment if you travel by car. Make a photocopy on both sides of all papers and cards you will take with you and keep a copy in a secure place preferably outside your home.	
43	Take with you the phone numbers to your local police and fire station as well as the local telephone service, your ISP, a 24-hour plumber, and any of the trusted people with access to your home.	
44	Get a UPS (uninterruptable power supply) for any computer systems which will stay running at home and make sure that they are set in the BIOS to reboot on power failure and boot on any error. An UPS will come in all shapes and sizes but get one that gives you at least 10 minutes of system running time with your monitor off.	
45	Get an UPS for any electronic systems you must have running while you are gone like your home security system central controller. They usually also have a battery back up but if it's less than 2 hours of reserve time get an UPS for it as well.	
46	Get a mobile phone back-up for your alarm. They don't cost much more and are a good alternative for a cut phone line.	
47	Test your home alarm system and sensor batteries and replace as necessary. Make sure to set your alarm system to arm anyway on error so even if a sensor is not responding, the system will trip from the other sensors.	
48	If you are taking your laptop, make sure you have some kind of dial-up access and spare phone cable to access the Internet if you rely on it. WiFi access problems can occur. You may not get direct Internet access. Dial-up is always nice to have when security failures occur. You may even consider getting a secure means to dial-in to your home computer system like a RAS (Remote Access Server) in case Internet access at your home is down.	

## Resilience

This is the control for Murphy's laws. When something goes wrong and the security or controls fail, then resilience assures that they break down in a way that is at least manageable and safer.

	TASK	COMPLETED
49	Make your main home alarm system console difficult to get to. Placing it in a room behind a locked door is a good start and not where it's often found-- just inside the front door. It shouldn't be in an obvious, reachable, smashable place.	
50	For very little money you can get a lot of these magnetic mini-alarms that go off if someone opens a door or window. They will often not tie in to your alarm system but they are loud and annoying if someone opens the door. Put them on the very low or very high inside of entry and major internal doors, even the front door but bear in mind you'll have to deal with the noise for a few seconds after you switch it on, slip out, and shut the door behind you.	

## Safety (Process)

*Safety process controls are passive. They don't need to act on an interaction to create a safer environment.*

## Non-repudiation

To repudiate is to refuse to acknowledge something happened such as to deny involvement in an incident. As a control, non-repudiation does not allow someone to refuse or deny anything because there is proof that it has happened and they were involved. This proof can be video footage, a written testament, or a credible eye witness.

	TASK	COMPLETED
51	A few cameras around the house, inside and out, recording to a unit locked away in a discrete place is ideal. Since most any wireless camera can often be viewed by anyone with a viewer for that frequency, it's wise not to use them inside your house or anywhere you expect privacy. Also, cheap cameras though get hot and the picture fades and blurs after a couple of days of continuous running. So be careful what you buy.	
52	Hidden cameras, the kind that look like books or objects, work well but if they are wireless they may have a short power life and may be trackable by a cheap gadget that the crooks can carry to find them. A better alternative may be an network-ready camera that you hide out of view and send the data stream to your computer for capture and remote monitoring if you can access your home PC over the Internet. To run the Ethernet cable back to your computer, consider using Ethernet over power lines which you can plug the first unit into the wall by the camera (a dual power jack will give both the power to the camera and take the network transmitter) and the other by your	

	computer's hub, switch, or router. Keep in mind, an attacker could plug into your outside electrical outlet and get on your home network so be sure that you can shut off those outer outlets or have them protected by passive infrared sensors.	
53	Leave a guestbook by the door to encourage thieves to sign-in upon entry along with their address and phone number to receive updates of when you get new valuables-- Just Kidding- but it would be nice if they fell for it, right?!	

## Confidentiality

Confidentiality is about protecting the message. The message can be transmitted in many ways such as speaking out loud, over the telephone, or via e-mail. To control the personal things that should not be shared to others is to assure that nobody else can understand the message if they listen in. There are many ways to make such information confidential such as speaking in an obscure foreign language for the region, using code words, and even encryption (like the "s" in https makes web transactions confidential).

	TASK	COMPLETED
54	Encrypt your data. Make an encrypted partition and lock up important stuff that you take with you. Lock up important stuff you have at home, even the stuff in the safe. Use a good pass-phrase that looks like something else so you can keep in your wallet. For example, "Walden Library 10/05" might be one you keep scribbled on a card in your wallet among other calendar items but is actually the pass-phrase for your encrypted partition.	
55	If you travel with a laptop, set your email client to use SPOP and SSH over SMTP while traveling. Actually, you should use those setting all the time anyway. Or at least use HTTPS web-based mail over the browser.	
56	If you have a babysitter staying with your children, leave the children with an emergency mobile phone on VIBRATE that they know is only for them to know about, is not a toy, and is only for emergencies in case they need to contact you in secret.	
57	If you have a house-sitter or babysitter remove all phones in your house except the corded, main one in the central house location usable only at a standing location. This way if you need to say something in private to your child on the phone, you can be sure the sitter is not likely listening on another line. Furthermore it will make it more likely the sitter will not have a comfortable location for chatting long periods on the phone.	

## Privacy

As a control, Privacy means that your actions cannot be seen or interpreted by anyone who is not supposed to know. When we attend a private party, it means that anyone who is not on the guest list is forbidden from seeing what goes on at that party. They might be able to hear the party but they cannot be sure who at the party is doing what at any time.

	TASK	COMPLETED
58	Don't leave an itinerary of your travels around in the house. Get rid of all vacation booklets or any details that says where you're going and when.	
59	Take down any agendas or calendars you have hanging around that have appointments in them or any other times when you will be out of the house and put them out of view.	
60	Clear your computer of unencrypted private data, clear your voice mails, change your answering machine tape and destroy the old one, and generally clean up unneeded stuff about yourself. If you are bringing a laptop or mobile phone, make sure they are clean of unencrypted personal items as well.	
61	Shred trash with personal data, including receipts. Lock away other papers with personal data in a secure cabinet. Remember that common desk and cabinet locks are easily broken.	
62	Remove your trash from the house and yard just before you leave to make sure the cans are all empty.	

## Integrity

Assuring Integrity is common in many ways where a parent makes sure what you have around the house to eat or drink does not get contaminated and harm you. It's also how you make sure that the state of the house you leave is the same upon your return.

	TASK	COMPLETED
63	Shut off your water main from inside the house if you can. Put away hoses and tubes outside. While thieves don't necessarily care about creating water damage, vandals do.	
64	Unplug all electronics you can including computers you don't need access to and disable as much from the main breaker as possible to prevent overloads, fires, and abuse from vandals.	
65	Clean up the house, and wash down the doors, frames, and windows. Put small rip stickers (like stores use for price tags) at the base of doors that even your trusted people should not be entering. If you are snooped or robbed you want to be able to notice that something is changed or out of place.	



## Alarm

An alarm is a control to make you aware that security has been circumvented or controls have been broken. An alarm can be immediate as in an alert or can be standing as in a record of the incident you check occasionally. Most important however is that if the alarm function does not inform you of the action for whatever reason then it fails to work as an alarm.

	TASK	COMPLETED
66	Anyone who has a key to your home may also need an alarm fob or alarm codes to remotely deactivate and reactivate your alarm if it goes off on purpose or accidentally. Make sure theirs is unique if you can so you can see in the logs later who it was.	
67	Make sure you are the first person that the alarm notifies, even before your hired security service or any trusted people watching the house for you. You should be able to know first and remotely control the alarm through the telephone when it calls. This also lets you verify that the security service is doing its job or that nobody left at home (like children or a house-sitter) is in any danger.	
68	Make sure your security sensor console can log interactions for the length of time you are gone. Some will even record sensor activity so you know exactly which sensor went off and when. For that to work, you need to have your sensors logically named and numbered so you know sensors 1, 2, and 3 are in the front yard and from left to right, etc.	
69	Give your your neighbor, house-sitters, security service, and banker your email and perhaps mobile phone number so they can check-in when things go wrong.	
70	If you can be notified immediately of all card charges, you should. Some will send an SMS with details of the charge after each charge. This way you will even be notified if a motel or restaurant double charges or over-charges you before you check-out so you can get your money back!	

## Appendix A - License

### The Open Methodology License 3.0

This license is Copyright under the Creative Commons 2.5 Attribution, 2007, ISECOM

#### PREAMBLE

This license is to protect a methodology as a complex set of methods, processes, or procedures to be applied within a discipline. The key requirements of this license is that 1) the methodology has value as intellectual property which through application thereof can produce value which is quantifiable and 2) that the methodology is available publicly and an appropriate effort is made for the methodology to be transparent to anyone.

With respect the GNU General Public License (GPL), this license is similar with the exception that it gives the right to software developers to include this open methodology license (OML) to software which is closed and distributed commercially.

The main concern covered by this license is that open methodology developers receive proper credit for contribution and development.

Special considerations to the Free Software Foundation and the GNU General Public License for legal concepts and wording.

#### TERMS AND CONDITIONS

1. The license applies to any methodology or other intellectual tool (ie. matrix, checklist, etc.) which contains a notice placed by the creator saying it is protected under the terms of this Open Methodology License 3.0.
2. The Methodology refers to any such methodology, intellectual tool or any such work based on the Methodology. A "work based on the Methodology" means either the Methodology or any derivative work by Trade Secret law which applies to a work containing the Methodology or a portion of it, either verbatim or with modifications and/or translated into another language.
3. All persons may use, distribute, teach, and promote the Methodology exactly as it has been received, in any medium, provided that they conspicuously and appropriately publish on each copy the appropriate Open Methodology License notice and the creator or creators of the Methodology; keep intact all the notices that refer to this License and to the absence of any warranty; give any other recipients of the Methodology a copy of this License along with the Methodology, and the location as to where they can receive an original copy of the Methodology from the Methodology creator.
4. Any persons who sell training, products, or services of the Methodology must clearly display the name of the creators of this Methodology in addition to the terms of this license.
5. All persons may include this Methodology in part or in whole in commercial service offerings, private or internal (non-commercial) use, or for educational purposes without explicit consent from the creator providing points 3 and 4 are complied with.
6. No persons may distribute an adaption, modification, or change of this Methodology without explicit consent from the creator.
7. All persons may utilize the Methodology or any portion of it to create or enhance commercial or free software, and copy and distribute such software under any terms, provided that they also meet all of these conditions:
  - a) Points 3, 4, 5, and 6 of this License are strictly adhered to.
  - b) Any reduction to or incomplete usage of the Methodology in software must strictly and explicitly state which parts of the Methodology were utilized in the software and which parts were not.
  - c) When the software is run, all software using the Methodology must either cause the software, when started running, to print or display an announcement of use of the Methodology including a notice of warranty how to view a copy of this License or make clear provisions in another form such as in documentation or delivered open source code.
8. If, as a consequence of a court judgment or allegation of Patent infringement, Trade Secret law infringement, or for any other

## HSM 1.2 - The Home Security Methodology Vacation Guide

legal reason, where conditions are imposed on any person (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse said person from the conditions of this License. If said person cannot satisfy simultaneously the obligations under this License and any other pertinent obligations, then as a consequence said person may not use, copy, apply, use, distribute, or promote, the Methodology at all. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

9. If the distribution and/or use of the Methodology is restricted in certain countries either by patents or by Trade Secret interfaces, the original creator who places the Methodology under this License may add an explicit geographical distribution limitation excluding those countries, so that application, use, or distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. ISECOM may publish revised and/or new versions of the Open Methodology License. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

### **NO WARRANTY**

11. Because the methodology is licensed free of charge, there is no warranty for the methodology, to the extent permitted by applicable law. except when otherwise stated in writing the creator and/or other parties provides the methodology "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance in use of the methodology is with the persons accepting this license. Should the methodology prove incomplete or incompatible said person assumes the cost of all necessary servicing, repair or correction.

12. In no event unless required by applicable law or agreed to in writing will the creator, or any other party who may use, apply, or teach the methodology unmodified as permitted herein, be liable to any persons for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the methodology (including but not limited to loss, inaccuracies, or failure of the methodology to operate with any other methodologies), even if such holder or other party has been advised of the possibility of such damages.



**SECURITY IS ALWAYS ABOUT PEOPLE.**

**ISECOM's security certifications  
are for you, your work, and those  
waiting for you at home.**

**ISECOM**  
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES  
**Making Sense of Security**

*Find out more at [www.isecom.org/training](http://www.isecom.org/training)*