# The GreyHat Group

## Preamble

Welcome to the constitution for the The Grey Hat Computing Group at the University Of Washington Tacoma. This document attempts to create a framework for membership, group organization, and constitutional bylaws.

## Article I. Name

1.1:  The Grey Hat Computing Group is the exact title to be used in addressing the organization, and is an organization of the University of Washington Tacoma

## Article II. Purpose

2.1: The Grey Hat Computing Group at the University Of Washington Tacoma is here to provide its members with a list of relevant topics to learn about the field of computer security,  and provide instructional tutorials in obtaining security tools used by industry professionals.

## Article III. Membership

3.1: Membership shall be organized into four groups.

3.1.2: Member: A member with voting rights.

3.1.3: Prospective member: Persons who have an interest in becoming a member but do not have voting rights and whose group rights are limited as outlined below.

3.1.4: Provisional Members: New members who have not fully completed the membership process.

3.2: Member: Becoming a member is a three step process. Once established as a member their rights are unrestricted.

3.2.1: A new member must have a trusted GPG or PGP style public encryption key. It must be signed and verified by at least two established members. It will be kept on file with the group and must have an expiration date less than or equal to 365 days from its creation date.

3.2.2: The new member must agree to the groups software licensing and nondisclosure agreement, as well as code of conduct. (herein referred to as the documents)

3.2.3: The new member will have to pay a lifetime membership fee of $5.00 (USD). If this cannot be afforded by the new member the board may reach consensus to suspend this requirement, for that member.

3.2.4: Prospective member: Defined as a person who is interested in becoming involved in the group. They may have come to a meeting or talked with other members but have not completed any steps to becoming a member. Their rights are restricted.

3.2.5: Provisional Member: Defined as a person who is in the process of becoming a full member.

3.3: Rights of Membership

3.3.1: Members have a vote. Members have access to protected group resources such as CVS repository, penetration server, group suffixed email address (@uwtgreyhat.org), access and usage of group GPG/PGP encryption keys. Unrestricted access to group publications and white papers. Members can also release software under the group name (in accordance with the license). Members can also appear at public functions as a representative of the group at large (in accordance with the code of conduct). Other rights may be defined as needed.

3.3.2: Rights of nonmembers or prospective members: These types of people have access to all publicly available resources like public publications and white papers. They can read only access group forums and contact members of the group if they wish.

3.3.3: Provisional members: Members who have not signed the documents have the same rights as nonmembers or prospective members, even if they have paid the membership dues and have a valid and signed GPG/PGP key. Provisional members who have signed the documents and have a valid and signed GPG/PGP key have all privileges

as full members but they do not have the right to vote. All other types of provisional members will be treated as prospective or nonmembers.

3.4: Discipline of membership

3.4.1: Members can be disciplined for any reason that the assembly of officers deems appropriate. This includes but is not limited to: malicious code use in the wild, penetrating servers that are not sponsored by the group, illegally gaining access to computing systems, releasing a security hole or exploit to the world at large without first contacting the company or organization that created the product.

3.4.2: To determine if a member needs to be disciplined all the officers must be present physically or electronically to hear the arguments. The prosecuting person will have 10 minutes to present the arguments for discipline. The defensive person will have 10 minutes to present the arguments against discipline. Then the prosecuting person will have 5 minutes to respond to the arguments presented by the defense. Then the defensive person will have 7 minutes to respond to the argument and response of the prosecuting person.

3.4.3: The officers will deliberate until they reach a verdict. The chair of the meeting may postpone deliberation until a later date if necessary. The verdict is made when a simple majority of the officers determines to vote for or against disciplinary action. If no majority can be reached in event of an even number of officers, the member with the most seniority present who is not an officer can be included in the vote to make it an odd number.

3.4.4: In the event that the offending party is an officer then the member with the most seniority who is not an officer will be included in the vote.

3.4.5: In the event that the offending party is the member with the most seniority then the member with the next most seniority will replace the member with the most seniority in all disciplinary proceedings.

3.4.6 Punishment actions include but are not limited to, revoking of any or all of the offending member’s rights as outlined in this document. Confiscation of written code and/or loss of ownership rights to written code, suspension from meetings, loss of voting rights, monetary fine to continue membership with the group, and expulsion from the group.

## Article IV. Officers

4.1: Officers: Full-fledged members who have been elected to office by a vote from the membership at large.

4.2: Officers responsibilities: Officers are elected to office by a consensus from the membership.

4.2.1: President: Responsible for the general health and vision of the group at large. Coordinates new/existing projects and other duties as assigned.

4.2.3: Vice President: Responsible for making sure new members are fully qualified. Responsible for recruitment. Acts as chair at meetings. Responsible for making sure that code written is credited to the right person. Other duties as assigned.

4.2.4: Secretary: Responsible for keeping meeting minutes. Responsible for maintaining group key ring web of trust. Responsible for updating and signing cryptographic keys and keeping track of all keys. Maintains all members signed documents. Other duties as assigned.

4.2.5: Treasurer: Responsible for group accounts and expenditures. Responsible for any fund raising. Other duties as assigned.

4.2.6: Marginalized Populations Initiative Officer (MPIO): Responsible for outreach to minority and women populations. Responsible for initiating diversity and internationalization/localization when possible. Other duties as assigned.

4.2.7: Chief Technical Officer (CTO): Responsible for maintaining all group servers. Maintains group website. Has “root” account on all servers. Specifically maintains (but not limited to) web server, penetration server, code base and knowledge base server. Other duties as assigned.

4.2.8: Academic/Industrial Liaison: Responsible for creating and maintaining relationship with the University and Industrial contacts. Specifically responsible for (but not limited to) inviting guest speakers from industry or academia. Initiating learning or curricula into technologies that have not been introduced into the group yet. Responsible for outlining membership's basic skill set. Responsible for making sure that membership meets standards for basic skill set.

## Article V. Requirement of meetings

5.1: The group is required to meet at least twice a year. The majority of the membership must be present either physically or electronically, for it to count.

5.2: Chair shall be handled by the Vice President, then President in their absence, then to Secretary, then Treasurer, then MPIO, then CTO, then Liaison, then to the member with most seniority.

5.3: Meetings shall be no less than 30 minutes, unless the membership comes to a consensus that this requirement may be temporarily suspended.

5.4: Meetings will start with introductions then move to reports from the various officers then to old business then to new business. Cryptographic key signings shall be done immediately after the meeting unless the chair decides that time can be allocated for it during the meeting. At least two officers must agree that there is sufficient need for key signings to allocate meeting time to it.

## Article VI. Software and source code licensing agreement

*6.1: Grey Hat Computing Group Software and Code Licensing Agreement*
All of the expressions of ideas pertaining to GHG that are fixed in any tangible medium such as digital and physical documents are protected by copyright law as embodied in title 17 of the United States Code. These expressions include the work product of both: your student colleagues and, your faculty advisors. Within the constraints of "fair use", you may copy these copyrighted expressions for your personal intellectual use in support of your education or activities with the group. Such fair use by you does not include further distribution by any means of copying, performance or presentation beyond the circle of your close acquaintances, student colleagues, faculty members and your family. If you have any questions regarding whether a use to which you wish to put one of these expressions violates the creator's copyright interests, please feel free to ask the advisor, copyright holder, or knowledgeable officer for guidance. In conjunction with copyright law as described in title 17 of the United States Code, I agree to be additionally bound by the following rights for all code that I author, that is developed within the group or for its operations, where Title 17 of the copyright law addresses the specific issues addressed below

Title 17 will supersede this agreement.
1. Any changes that I make to the licensing scheme or any restrictions that I place on my code will not be able to, in any way, violate this agreement.
2. Any code that I create that is used in an application or library that is released by the group to the public at large, therefore becoming a “public release” can be released under the GPL, LGPL or other Open Source recognized license agreement. At such time this agreement will become null and void.
3. The group will retain rights under “fair use” guidelines for its intellectual and academic use. In other words the group has the right to make my code available to members for learning purposes. The group however is specifically prohibited from making any financial profit by use of the code unless a written agreement exists from the code's copyright holder to allow the group to do so.
4. If I use my code in an intentionally malicious manner or if I have been disciplined for malicious code use by the group. I agree that I will forfeit all rights to any code that I have created.
5. I agree that I will hold the group and by extension UWT harmless for any legal or personal repercussions that my code has. Especially if I use my code as a virus or for attacking a distributed network system.
6. I agree to be bound by the terms of this agreement even if I am no longer a part of the membership of GHG.
Personally signed by me _____ this _____ day of _____ in the year _____.
Signed _____
Witness _____

## Article VII. Nondisclosure agreement

*7.1: Grey Hat Computing Group Nondisclosure Agreement*
To support an academic environment of rigorous discussion and open expression of personal thoughts and feelings, we, as members of the academic community, must be committed to the inviolate right of privacy of our student and instructor colleagues. As a result, we must not share personally identifiable information about any member of our community including information about the ideas they express, their families, life styles and their political and social affiliations. If you have any questions regarding whether a disclosure you wish to make regarding anyone in the group or in the GHG community violates that person's privacy interests, please feel free to ask the advisor or responsible officer for guidance. Knowing violations of these principles of academic conduct, privacy or copyright may result in University disciplinary action under the Student Code of Conduct. Please familiarize yourself with the University of Washington's Student Code of Conduct at:
http://www.washington.edu/students/handbook/conduct.html

Additionally, I _____ agree to be bound by the following terms of this nondisclosure agreement:
1. I agree to keep all “zeroday” exploits known or discovered contained to within the protected knowledge base of the group until the proper company or organization has been notified and given sufficient time to respond.
2. I agree to keep all electronic or actual transmission of sensitive code and sensitive group discourse encrypted to only be viewable by the recipient or recipients.
3. I agree to keep all passwords and sensitive knowledge protected to the best of my abilities.
4. I agree that any and all code in development by me or other members of the group that is sensitive in nature or not ready for public release will be closed source which means that I will discuss it only with members and certain appointees, appointed by the officers who have access to the source code.
Personally signed by me _____ this _____ day of _____ in the year _____.
Signed _____
Witness _____

## Article VIII. Code of conduct

8.1 Grey Hat Computing Group Code of Conduct
Students who are members of the Grey Hat Group are trusted with access to the practices, procedures and technologies used to attack and protect valuable information assets and systems. This trust requires an uncompromising commitment to satisfying the highest moral and ethical standards. Adherence to all laws, rules and regulations applicable to the field and practice of information security is critical. However, this commitment requires more than simple obedience to the law. Our faculty, as well as advisors, and fellow student members expect that persons involved with the GHG will demonstrate sound ethics, honesty and fairness in in all their security related endeavors.
GHG understands that this code must be flexible enough to deal with hundreds of different daily activities in addition to future academic and business issues. Toward that end, GHG expects each student member to use sound judgment in the performance of his/her involvement.
Sound judgment means, among other things, that the student member should consider whether his/her conduct would be viewed with approval by family, friends, colleagues and the community at large were the activity is to be disclosed. Students should read this code carefully, and then execute the attached form to certify that they have done so and to acknowledge a commitment to follow its terms.
1. Student members are responsible for behaving according to the highest standards of ethical conduct, for conducting themselves in conformance with all laws of the United States and other jurisdictions in which they may find themselves, and for exercising due diligence in the conduct of their participation and projects within GHG.
2. Student members should be aware that they may be held personally liable for any improper or illegal acts committed during the course of their involvement with the group, and that "ignorance of the law" is not a defense. Student members may be subject to civil penalties, such as fines, or regulatory sanctions, including suspension or expulsion. Potential penalties for illegal acts under federal sentencing guidelines are severe and may include imprisonment and substantial monetary fines. Existing federal and state laws, as well as the laws of foreign jurisdictions, may impose civil money penalties, permit the issuance of cease and desist orders, or have other consequences.
3. Student members who are uncertain about the laws of a particular jurisdiction or whether certain acts or practices comply with the law should contact their advisor or group officer.
4. Student members who become aware of any violations of the law or questionable practices by a fellow members should also contact their advisor or an officer immediately. Disclosure of questionable or improper conduct to proper members who can take appropriate action is critical to the group's success. All such communications will be investigated fully. Moreover, retribution against student members who report ethics complaints or member misconduct will not be tolerated and is itself a violation of the ethical standards.
5. Student members are responsible for understanding that it is both illegal and unethical to engage in practices that violate copyright laws or licensing arrangements. All GHG members must respect the rights conferred by such laws and arrangements and refrain from cracking copyright protection schemes, attempting to circumvent rights management software and making unauthorized copies of protected materials, including but not limited to, articles, documents and computer software.
6. Each student member must:

- Conduct activities in accordance with high ethical and moral standards.
- Conduct all activities in accordance with the academic integrity standards posted on the following University of Washington web site: http://www.washington.edu/computing/rules/
- Be aware of, and abide by, the laws of the United States, the individual States, foreign countries and other jurisdictions in which the student may conduct studies, projects, research or other activities
- Adhere to the spirit of the law as well as its substance

- Always act with personal integrity based on principles of sound judgment
- Neither condone nor ignore any illegal or unethical acts for any reason

Personally signed by me _____ this _____ day of _____ in the year _____.
Signed _____
Witness _____