2018 ACM Code of Ethics and Professional Conduct: Draft ~~2~~	**2018 ACM Code of Ethics and Professional Conduct: Draft *3***
Draft ~~2~~ was developed by The Code 2018 Task Force. (It is based on the 2018 ACM Code of Ethics and Professional Conduct: Draft ~~1~~)	Draft *3* was developed by The Code 2018 Task Force. (It is based on the 2018 ACM Code of Ethics and Professional Conduct: Draft *2*)
Preamble The ACM Code of Ethics and Professional Conduct ("the Code") ~~identifies key elements of ethical conduct in computing.~~	**Preamble** *The actions of computing professionals directly impact significant aspects of society. In order to meet their responsibilities, computing professionals must always support the public good.*[1] The ACM Code of Ethics and Professional Conduct ("the Code") *reflects this obligation by expressing the conscience of the profession and provides guidance to support ethical conduct of all computing professionals.*
The Code is designed to support all computing professionals, ~~which is taken to mean~~ current ~~or~~ aspiring computing practitioners ~~as well as those~~ who influence ~~their professional development~~, and those who use technology in an impactful way. The Code includes	The Code is designed to support all computing professionals, *including* current *and* aspiring computing practitioners, *instructors*, influencers, and *anyone* who uses technology in an impactful way. *Additionally, the Code serves as a basis for remediation when*

[1] Putting this first emphasizes that it is the highest principle and main purpose of the Code.

principles formulated as statements of responsibility, based on the understanding that the public good is always ~~a~~ primary consideration.	*violations occur.*[2] The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always *the* primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist *computing professionals* in understanding and applying *the principle*.
Section 1 outlines fundamental ethical ~~considerations~~. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 pertains ~~more specifically~~ to individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member and principles involving compliance with the Code are given in Section 4.	Section 1 outlines fundamental ethical *principles that form the basis for the remainder of the Code*. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 pertains to individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member, and principles involving compliance with the Code are given in Section 4.
The Code as a whole is concerned with how fundamental ethical principles apply to ~~one's~~ conduct ~~as a~~ computing professional. Each principle is supplemented by guidelines, which provide explanations to assist ~~members~~ in understanding and applying ~~it~~. ~~These extraordinary ethical responsibilities of computing professionals are derived from broadly accepted ethical principles.~~	The Code as a whole is concerned with how fundamental ethical principles apply to *a* computing professional's conduct.
The Code is not an algorithm for solving ethical problems, rather it ~~is intended to~~ serve as a basis for ethical decision making ~~in the conduct of professional work~~. ~~Words and phrases in a code of ethics are subject to varying~~	The Code is not an algorithm for solving ethical problems; rather it serves as a basis for ethical decision making. *When thinking through a particular issue, a computing professional may find that multiple principles should be taken into*

[2] Reworded, but brought up from last sentence of the Preamble in version 2.

~~interpretations, and a particular principle may seem to conflict with other principles in specific situations.~~ Questions related to these kinds of ~~conflicts~~ can best be answered by thoughtful consideration of the fundamental ethical principles, understanding the public good is the paramount consideration. The entire profession benefits when the ethical decision making process is transparent to all stakeholders. ~~In addition, it may serve as a basis for judging the merit of a formal complaint pertaining to a violation of professional ethical standards.[3]~~	*account, and that different principles will have different relevance to the issue.* Questions related to these kinds of *issues* can best be answered by thoughtful consideration of the fundamental ethical principles, understanding *that* the public good is the paramount consideration. The entire *computing* profession benefits when the ethical decision making process is accountable to and transparent to all stakeholders. *Open discussions about ethical issues promotes this accountability and transparency.*
1. GENERAL MORAL PRINCIPLES *A computing professional should...* **1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.**	**1. GENERAL MORAL PRINCIPLES.** *A computing professional should...* **1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.**
This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect diversity.	This principle, concerning the quality of life of all people, affirms an obligation *of computing professionals to use their skills for the benefit of society, its members, and the environment surrounding them*. *This obligation includes promoting* fundamental human rights and protecting each individual's right to autonomy in day-to-day decisions[4].

[3] Moved up, see previous footnote.
[4] Moved up from 3.5 in Draft 2.

An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. Computing professionals should ~~give consideration to whether the products~~ of their efforts will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work. When the interests of multiple groups conflict the needs of the least advantaged should be given increased attention and priority. In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should ~~be alert to, and make others aware of, any potential harm to the local or global environment~~.	An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. Computing professionals should *consider whether the results* of their efforts respect diversity, will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work. When the interests of multiple groups conflict, the needs of the least advantaged should be given increased attention and priority. In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should *promote environmental sustainability both locally and globally*.
1.2 Avoid harm. In this document, "harm" means negative consequences to any stakeholder, especially when those consequences are significant and unjust. Examples of harm include unjustified ~~death~~, unjustified ~~loss~~ of information, and unjustified damage to property, reputation, or the environment. This list is not exhaustive.	**1.2 Avoid harm.** In this document, "harm" means negative consequences to any stakeholder, especially when those consequences are significant and unjust. Examples of harm include unjustified *physical or mental injury*, unjustified *destruction or disclosure* of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive.
Well-intended actions, including those that accomplish assigned duties, may ~~unexpectedly~~ lead to harm. ~~In such an~~	Well-intended actions, including those that accomplish assigned duties, may lead to harm. *When that harm is*

~~event~~, those responsible are obligated to undo or mitigate the harm as much as possible. Avoiding ~~unintentional~~ harm begins with careful consideration of potential impacts on all those affected by decisions.	*unintended*, those responsible are obligated to undo or mitigate the harm as much as possible. Avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. *When harm is an intentional part of the system, those responsible are obligated to ensure that the harm is ethically justified and to minimize unintended harm*.[5]
To minimize the possibility of indirectly harming others, computing professionals should follow generally accepted best practices ~~for system design, development, and testing~~[6]. Additionally, the consequences of emergent systems and data aggregation should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.	To minimize the possibility of indirectly harming others, computing professionals should follow generally accepted best practices. Additionally, the consequences of emergent systems and data aggregation should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.
~~At work,~~ a computing professional has an additional obligation to report any signs of system risks that might result in ~~serious personal or social~~ harm. If ~~one's superiors~~ do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, ~~the~~ computing professional should thoroughly assess all relevant aspects ~~of the incident as outlined in Principle 2.5~~.	A computing professional has an additional obligation to report any signs of system risks that might result in harm. If *leaders* do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, *a* computing professional should thoroughly assess all relevant aspects.
1.3 Be honest and trustworthy.	**1.3 Be honest and trustworthy.**

[5] Added to make clear that the Code does not prohibit working in the defense industry.

[6] Removed to make this more generally applicable, not just restricted to these three areas.

Honesty is an essential component of trust. A computing professional should be ~~fair and~~ not make deliberately false or misleading claims and ~~should~~ provide full disclosure of all pertinent system limitations and potential problems. Fabrication of data, falsification of data, and ~~scientific mis~~conduct are ~~similarly~~ violations of the Code. ~~One who is professionally dishonest is accountable for any resulting harm.~~	Honesty is an essential component of trust. A computing professional should be *transparent* and provide full disclosure of all pertinent system limitations and potential problems. Making deliberately false or misleading claims, fabricating or falsifying data, and *other dishonest* conduct are violations of the Code.
~~A~~ computing professional should be honest about ~~his or her own~~ qualifications, and about any limitations in competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to conflicts of interest or otherwise tend to undermine the independence of their judgment.	Computing professionals should be honest about their qualifications, and about any limitations in competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to conflicts of interest or otherwise tend to undermine the independence of their judgment.
~~Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member should exercise care not to misrepresent ACM, or positions and policies of ACM or any ACM units.~~	*Computing professionals often belong to organizations associated with their work. They should not misrepresent any organization's policies or procedures, and should not speak on behalf of an organization unless authorized to do so.*[7]
1.4 Be fair and take action	**1.4 Be fair and take action**

[7] Same intent as before, but rewritten to apply more broadly.

not to discriminate.	**not to discriminate.**
The values of equality, tolerance, respect for others, and ~~equal~~ justice govern this principle. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of ~~ACM policy~~. Sexual harassment is a form of discrimination that limits fair access to the spaces where ~~the~~ harassment takes place.	The values of equality, tolerance, respect for others, and justice govern this principle. *Computing professionals should strive to build diverse teams and create safe, inclusive spaces for all people, including those of underrepresented backgrounds.* Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, *labor union membership*, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of *the Code. Harassment, including* sexual harassment, is a form of discrimination that limits fair access to the *virtual and physical* spaces where *such* harassment takes place.
Inequities between different groups of people may result from the use or misuse of information and technology. Technologies should be as inclusive and accessible as possible. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.	Inequities between *individuals or* different groups of people may result from the use or misuse of information and technology. Technologies *and practices* should be as inclusive and accessible as possible. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.
1.5 Respect the work required to produce new ideas, inventions, and other creative and computing artifacts.	**1.5 Respect the work required to produce new ideas, inventions, creative *works*, and computing artifacts.**

~~The development of~~ new ideas, inventions, ~~and other~~ creative and computing artifacts creates value for society, and those who expend ~~the~~ effort needed for this should expect to gain value from their work. Computing professionals should therefore provide appropriate credit to the creators of ideas or work. This may be in the form of respecting authorship, copyrights, patents, trade secrets, ~~non-disclosure agreements~~, license agreements, or other methods of ~~attributing~~ credit where it is due.	*Developing* new ideas, inventions, creative *works*, and computing artifacts creates value for society, and those who expend *this* effort should expect to gain value from their work. Computing professionals should, therefore, provide appropriate credit to the creators of ideas or work. This may be in the form of respecting authorship, copyrights, patents, trade secrets, license agreements, or other methods of *assigning* credit where it is due.
Both custom and the law recognize that some exceptions to a creator's control of a work are necessary ~~to facilitate~~ the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works. Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and other work put into the public domain. Computing professionals should avoid misappropriation of ~~a commons~~.	Both custom and the law recognize that some exceptions to a creator's control of a work are necessary *for* the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works. Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and other work put into the public domain. *Some work contributes to or comprises shared community resources*. Computing professionals should avoid misappropriation of *these resources*.
1.6 Respect privacy. ~~"Privacy" is a multi-faceted concept and~~ a computing professional should become	**1.6 Respect privacy.** *The responsibility of respecting privacy applies to computing professionals in a*

conversant in its various definitions and forms.	*particularly profound way. Therefore,* a computing professional should become conversant in privacy's various definitions and forms.
Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected.	Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected.
Computing professionals should use personal data only for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals or groups. Computing professionals should establish procedures that allow individuals to review their personal data, correct inaccuracies, and opt out of automatic data collection.	Computing professionals should only use personal data for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent unauthorized data collection, ensuring the accuracy of data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to give informed consent to automatic data collection, review their personal data, correct inaccuracies, and, where appropriate, remove data.
Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined and enforced, and personal information gathered for a specific purpose should not be used for other purposes without consent ~~of the individual(s)~~. When data collections are merged, computing professionals should take special care for privacy. Individuals may be readily identifiable when several data collections are merged, even though those individuals are not identifiable in	Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and *communicated to data subjects*. Personal information gathered for a specific purpose should not be used for other purposes without *the person's* consent. Computing professionals should take special care for privacy when data collections are merged. Individuals *or groups* may be readily identifiable when several data collections are merged, even

any one of those collections in isolation.	though those individuals *or groups* are not identifiable in any one of those collections in isolation.
1.7 Honor confidentiality.	**1.7 Honor confidentiality.**
Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code. User data observed during the normal duties of system operation and maintenance should be treated with strict confidentiality, except in cases where it is evidence for the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities, and the computing professional should consider thoughtfully whether such disclosures are consistent with the Code.	Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code. User data observed during the normal duties of system operation and maintenance should be treated with strict confidentiality, except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities, and a computing professional should consider thoughtfully whether such disclosures are consistent with the Code.
2. PROFESSIONAL RESPONSIBILITIES *A ~~practicing~~ computing professional should...*	**2. PROFESSIONAL RESPONSIBILITIES.** *A computing professional should...*
2.1 Strive to achieve ~~the~~ high~~est~~ quality in both the process and products of professional work.	**2.1 Strive to achieve high quality in both the process and products of professional work.**

Computing professionals should insist on high quality work from themselves and from colleagues. This includes respecting the dignity of employers, colleagues, clients, users, and anyone affected either directly or indirectly by the work. ~~High quality process includes~~ an obligation to keep the client or employer properly informed about progress toward completing ~~that project~~. Professionals should be cognizant of the serious negative consequences that may result from poor quality and should resist any inducements to neglect this responsibility.	Computing professionals should insist on high quality work from themselves and from colleagues. This includes respecting the dignity of employers, colleagues, clients, users, and anyone *else* affected either directly or indirectly by the work. *Computing professionals have* an obligation to keep the client or employer properly informed about progress toward completing *the work*. Professionals should be cognizant of the serious negative consequences *affecting any stakeholder* that may result from poor quality *work* and should resist any inducements to neglect this responsibility.
2.2 Maintain high standards of professional competence, conduct, and ethical practice. High quality computing depends on individuals and teams who take personal and ~~organizational~~ responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and awareness of the social context in which the work may be deployed. Professional competence also requires skill in reflective analysis for recognizing and navigating ethical challenges. Upgrading necessary skills should be ongoing and	**2.2 Maintain high standards of professional competence, conduct, and ethical practice.** High quality computing depends on individuals and teams who take personal and *group* responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and with awareness of the social context in which the work may be deployed. Professional competence also requires skill in reflective analysis and in recognizing and navigating ethical challenges. Upgrading necessary skills should be ongoing and

should include independent study, conferences, seminars, and other informal or formal education. Professional organizations, ~~including ACM, are committed to~~ encouraging and facilitating those activities.	should include independent study, conferences, seminars, and other informal or formal education. Professional organizations *and employers should* encourage and facilitate those activities.
2.3 Know, respect, and apply existing ~~laws~~ pertaining to professional work. ~~ACM members must~~ obey existing regional, national, and international laws unless there is a compelling ethical justification not to do so. Policies and procedures of the organizations in which one participates must also be obeyed, but compliance must be balanced with the recognition that sometimes existing laws and rules are immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.[8]	**2.3 Know, respect, and apply existing *rules* pertaining to professional work.** *"Rules" here includes* regional, national, and international laws and regulations, as well as any policies and procedures of the organizations *to which the professional belongs*. Computing professionals must obey these rules unless there is a compelling ethical justification to do otherwise. Rules that are judged unethical should be challenged. *A rule may be unethical when it* has an inadequate moral basis, it is superseded by another rule, or it causes recognizable harm that could be mitigated through its violation. A computing professional who decides to violate a rule because it is unethical, or for any other reason, must consider potential consequences and accept responsibility for that action.

[8] The changes in this section are such that the diff is not interesting to look at. The basic intention of the section has been maintained, but it has been substantially re-written for readability and clarity.

2.4 Accept and provide appropriate professional review. Quality professional work in computing depends on professional reviewing and critiquing. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical review of the work of others.	**2.4 Accept and provide appropriate professional review.** *High* quality professional work in computing depends on professional review *at all stages*. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical reviews of other's work.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks. Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives.	**2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.** Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives.
Computing professionals are in a position of ~~special~~ trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. Extraordinary care	Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. Extraordinary care

should be taken to identify and mitigate potential risks in self-changing systems. ~~Systems whose~~ future risks ~~are unpredictable~~ require frequent reassessment of risk as the system ~~develops~~ or should not be deployed. ~~When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in Principle 1.3.~~ ~~As noted in the guidance for Principle 1.2 on avoiding harm, any signs of danger from systems should be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for Principle 1.2 for more details concerning harm, including the reporting of professional violations.~~	should be taken to identify and mitigate potential risks in self-changing systems. *A system for which* future risks *cannot be reliably predicted* requires frequent reassessment of risk as the system *evolves in use,* or it should not be deployed. *Any issues that might result in major risk should be reported.*
2.6 ~~Accept only those responsibilities for which you have or can obtain the necessary expertise, and honor those commitments.~~	**2.6 Have the necessary expertise, or the ability to obtain that expertise, for completing a work assignment before accepting it. Once accepted, that commitment should be honored.**
~~A computing professional has a responsibility to evaluate every potential work assignment. If the professional's evaluation reveals that the project is infeasible, or should not be attempted for other reasons, then the professional should disclose this to the employer or client, and decline to attempt the assignment in its current form.~~	A computing professional is accountable for evaluating potential work assignments.

Once it is decided that a project is feasible and advisable, the professional should make a judgment about whether the project is appropriate to the professional's expertise. If the professional does not currently have the expertise necessary to complete the project the professional should disclose this shortcoming to the employer or client. The client or employer may decide to pursue the project with the professional after time for additional training, to pursue the project with someone else who has the required expertise, or to forego the project.	Once it is decided that a project is feasible and advisable, the professional should make a judgment about whether the work assignment is appropriate to the professional's expertise. If the professional does not currently have the expertise necessary to complete the assignment, the professional should disclose this shortcoming to the employer or client. The client or employer may decide to pursue the assignment with the professional after time for additional training, to pursue the assignment with someone else who has the required expertise, or to forego the assignment.
~~The major underlying principle here is the obligation to accept personal accountability for professional work~~. The computing professional's ethical judgment should be the final guide in deciding whether to ~~proceed~~.	A computing professional's ethical judgment should be the final guide in deciding whether to *work on the assignment*.
2.7 Improve public understanding of computing, related technologies, and their consequences.	**2.7 Improve public *awareness and* understanding of computing, related technologies, and their consequences.**
Computing professionals ~~have a responsibility to~~ share technical knowledge with the public ~~by creating~~ awareness and encouraging understanding of computing, including the impacts of computer systems, their limitations, their vulnerabilities, and opportunities that they present. ~~This imperative implies an obligation to~~ counter any false views related to	Computing professionals *should* share technical knowledge with the public, *foster* awareness *of computing*, and encourage understanding of computing. *Important issues include* the impacts of computer systems, their limitations, their vulnerabilities, and opportunities that they present. *Additionally, a computing professional should* counter false views

computing.	related to computing.
2.8 Access computing and communication resources only when authorized to do so.	**2.8 Access computing and communication resources only when authorized to do so.**
~~This principle derives from Principle 1.2 - "Avoid harm to others."~~ No one should access~~ or use~~ another's computer system, software, or data without permission. ~~One~~ should have appropriate approval before using system resources, unless there is an overriding concern for the public good. To support this ~~clause~~, a computing professional should take appropriate action to secure resources against unauthorized use. Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code~~ (such as Principle 1.4)~~.	No one should access another's computer system, software, or data without permission. *A computing professional* should have appropriate approval before using system resources unless there is an overriding concern for the public good. To support this *principle*, a computing professional should take appropriate action to secure resources against unauthorized use. Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code.
	2.9 Design and implement systems that are robustly and usably secure.[9] *Breaches of computer security cause harm. It is the responsibility of computing professionals to design and implement systems that are robustly secure. Further,*

[9] New principle addressing cybersecurity and the importance of usability in designing security.

	security precautions are of no use if they cannot or intentionally will not be used appropriately by their intended audience in practice; for example, if those precautions are too confusing, too time consuming, or situationally inappropriate. Therefore, the design of security features should make usability a priority design requirement.
3. PROFESSIONAL LEADERSHIP PRINCIPLES In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. These principles generally apply to organizations and groups, as well as their leaders. *A computing professional acting as a leader should...*	**3. PROFESSIONAL LEADERSHIP PRINCIPLES.** In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. These principles generally apply to organizations and groups, as well as their leaders. *A computing professional acting as a leader should...*
3.1 Ensure that the public good is ~~a~~ central concern during all professional computing work. The needs of people—including users, ~~other people~~ affected directly and indirectly, customers, and colleagues—should always be a central concern in professional computing. Tasks associated with requirements, design, development, testing, validation, deployment, maintenance, ~~end-of-life processes~~, and disposal should have the public good as an explicit criterion for quality. Computing professionals should	**3.1 Ensure that the public good is *the* central concern during all professional computing work.** The needs of people—including users, *those* affected directly and indirectly, customers, and colleagues—should always be a central concern in professional computing. Tasks associated with requirements analysis, design, development, testing, validation, deployment, maintenance, *retirement*, and disposal should have the public good as an explicit criterion for quality. Computing professionals should keep this

keep this focus no matter which methodologies or techniques they use in their practice.	focus no matter which methodologies or techniques they use in their practice.
3.2 Articulate, encourage acceptance of, and evaluate fulfillment of the social responsibilities of members of an organization or group. Technical organizations and groups affect ~~the public at large~~, and their leaders should accept responsibilities ~~to society~~. Organizational procedures and attitudes oriented toward quality, transparency, and the welfare of society ~~will~~ reduce harm to ~~members of~~ the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation in meeting social responsibilities and discourage tendencies to do otherwise.	**3.2 Articulate, encourage acceptance of, and evaluate fulfillment of the social responsibilities of members of an organization or group.** Technical organizations and groups affect *broader society*, and their leaders should accept *the associated* responsibilities. Organizational procedures and attitudes oriented toward quality, transparency, and the welfare of society reduce harm to the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation *of all computing professionals* in meeting social responsibilities and discourage tendencies to do otherwise.
3.3 Manage personnel and resources to ~~design and build systems that~~ enhance the quality of working life.	**3.3 Manage personnel and resources to enhance the quality of working life.**
Leaders ~~are responsible for ensuring that systems~~ enhance, not degrade, the quality of working life. ~~When implementing a system,~~ leaders should	Leaders *should ensure that management* enhances, not degrade, the quality of working life. Leaders should consider the personal and professional development,

consider the personal and professional development, accessibility, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be ~~considered in system design and~~ in the workplace.	accessibility *requirements*, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be *used* in the workplace.
~~3.4 Establish appropriate rules for authorized uses of an organization's computing and communication resources and of the information they contain.~~[10]	
Leaders should ~~clearly define appropriate and inappropriate uses of organizational computing resources. These rules should be~~ clearly and effectively communicated to ~~those using their computing resources~~. In addition, leaders should ~~enforce those rules~~, and take appropriate action when they are violated. **3.5 Articulate, apply, and support policies ~~that protect the dignity of users and others affected by computing systems and related technologies~~.** ~~Dignity is the principle that all humans are due respect.~~ This includes the general	**3.4 Articulate, apply, and support policies *and processes that reflect the principles in the Code*.** Leaders should *ensure that organizational policies are consistent with the ethical principles in the Code, are* clearly defined, and are effectively communicated *to all stakeholders.* In addition, leaders should *encourage and reward compliance with those policies*, and take appropriate action when policies are violated. *Leaders should verify that processes used in the development of systems protect the public good and promote the dignity and autonomy of users. Designing or implementing processes that*

[10] 3.4 and 3.5 have been combined and simplified, and now emphasize that leaders are responsible for ensuring organizational policies and procedures are consistent with the Code.

public's right to autonomy in day-to-day decisions.[11] ~~Designing or implementing systems that deliberately or inadvertently violate, or tend to enable the violation of, the dignity or autonomy of individuals or groups is ethically unacceptable. Leaders should verify that systems are designed and implemented to protect dignity.~~	*deliberately or inadvertently violate, or tend to enable the violation of, the Code's principles is ethically unacceptable.*
3.6 Create opportunities for members of the organization and group to learn, ~~respect~~, and be accountable for the ~~principles~~, limitations, and impacts of systems. ~~This principle complements Principle 2.7 on public understanding.~~ Educational opportunities are essential ~~to facilitate optimal participation of~~ all organization or group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties, including experiences that familiarize them with the consequences and limitations of particular types of systems. Professionals should know the dangers of oversimplified models, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and the contexts in which they are deployed, and other issues related to the complexity of their	**3.5 Create opportunities for members of the organization or group to learn and be accountable for the *scope, functions*, limitations, and impacts of systems.** Educational opportunities are essential for all organization and group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties. *These opportunities should* include experiences that familiarize *computing professionals* with the consequences and limitations of particular types of systems. *Computing* professionals should *be fully aware of* the dangers of oversimplified models, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and the contexts in which they are deployed, and other issues related to the complexity of their

[11] Moved up to the guidance for 1.1.

profession.	profession.
	3.6 Retire legacy systems with care.[12] *Computing systems should be retired when it is judged impractical to continue supporting them. System developers should take care when discontinuing support for systems on which people still depend. Developers should thoroughly investigate viable alternatives to removing support for a legacy system. If these alternatives are not practical or unacceptably risky, the developer should assist stakeholders' graceful migration from the system to an alternative. When system support ends, stakeholders should be notified of the risks of their continued use of the unsupported system.* *System users should continually monitor the operational viability of their computing systems, accepting the timely replacement of inappropriate or outdated systems. The primary consideration must be the impact on stakeholders, who should be kept informed at all times.*

[12] Addresses concerns about the impact of abandoned systems.

3.7 Recognize when computer systems are becoming integrated into the infrastructure of society, and adopt an appropriate standard of care for those systems and their users.	**3.7 Recognize when a computer system is becoming integrated into the infrastructure of society, and adopt an appropriate standard of care for that system and its users.**
Organizations and groups occasionally develop systems that become an important part of the infrastructure of society. Their leaders have a responsibility to be good stewards of ~~that commons. Part of that stewardship requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, there are likely to be changes in the ethical responsibilities of the organization. Leaders of important infrastructure services should provide due process with regard to access to these services.~~ Continual monitoring of how society is using a product will allow the organization to remain consistent with their ethical obligations outlined in the principles of the code. ~~Where such standards of care do not exist, there may be a duty to develop them.~~	When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have a responsibility to be good stewards of *these socially integrated systems. Part of that stewardship requires establishing policies for fair system access, including for those who may have been excluded. That stewardship also requires that computing professionals monitor the level of integration of their systems into the infrastructure of society.* Continual monitoring of how society is using a system will allow the organization or group to remain consistent with their ethical obligations outlined in the Code. *As the level of adoption changes, there are likely to be changes in the ethical responsibilities of the organization or group. When appropriate standards of care do not exist, computing professionals have a duty to ensure they are developed.*
4. COMPLIANCE WITH THE CODE	**4. COMPLIANCE WITH THE CODE.**

A computing professional should... **4.1 Uphold, promote, and respect the principles of the Code.** The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles ~~expressed in~~ the Code. Each ACM member should encourage and support adherence by all computing professionals.	*A computing professional should...* **4.1 Uphold, promote, and respect the principles of the Code.** The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles of the Code. Each ACM member should encourage and support adherence by all computing professionals *regardless of ACM membership*.
Computing professionals who recognize breaches of the Code should take whatever actions are within their power to resolve the ethical issues they recognize. **4.2 Treat violations of the Code as inconsistent with membership in ACM.** ~~If an ACM member does not follow the Code, membership in ACM may be terminated.~~	**4.2 Treat violations of the Code as inconsistent with membership in *the* ACM.** Computing professionals who recognize breaches of the Code should take actions to resolve the ethical issues they recognize, *including, when reasonable, expressing their concern to the person or persons thought to be violating the Code. Possible actions also include reporting the violation to the ACM, which may result in remedial action by the ACM up to and including termination of the violator's ACM membership.*[13]

[13] Adds a duty to act as part of the guidance for this principle.