Privacy Policy

Revised to remove obsolete use of "affiliate", 6 December 2013
Prior version, February 27, 2002

Purpose

This policy informs network users what sensitive, confidential, or personally identifiable information is collected by Merit Network, Inc. (Merit), how long that information is kept, what the collected information is used for, what protections are in place to safeguard the information from inappropriate use or release, and under what circumstances the collected information may be released to third parties.

Philosophy

Merit is committee to protecting the privacy of all users of its networks, host computers, products, and services. Merit wants to contribute and to help others contribute to providing a safe and secure environment for all network users. Merit will always operate its networks, host computers, other systems, products, and services in ways that allow Merit and its Members to follow applicable laws and regulations regarding privacy and the collection, storage, and release of sensitive, confidential, or personally identifiable information.

To the greatest degree possible, Merit acts as the temporary custodian rather than the owner of information that passes across the networks and systems that it operates. Merit's Members and other users are almost always in a better position than Merit to make decisions about the disclosure of information to third parties and the laws and regulations (e.g., FERPA, HIPAA, ECPA, Michigan's Library Privacy Act-see below for more information) that may prohibit or allow such disclosure.

Merit is subject to and this privacy policy is based on the terms of the Merit Acceptable Use Policy which states in part that:

Users must respect the privacy of others....

and

Merit will not monitor or judge the content of information transmitted over Merit's network, but will investigate complaints of possible inappropriate use. In the course of investigating complaints, Merit staff will safeguard the privacy of all parties and will themselves follow the guidelines given in this [Acceptable Use] policy. Merit will only release sensitive, confidential or personally identifiable information to third parties when required by law or when in Merit's judgment release is required to prevent serious injury or harm that could result from violation of this [Acceptable Use] policy.

Scope

This policy applies to all sensitive, confidential, or personally identifiable information that is or can be collected from networks, host computers, or other equipment or systems provided, managed and controlled by Merit or by organizations performing work on Merit's behalf.

More specific privacy policies or statements may exist for specific host computers, systems, products, or services provided, managed, and controlled by Merit. When such privacy policies or statements exist, they will be consistent with this policy.

This policy does not apply to networks, host computers, other equipment, or systems that are managed or controlled by Merit's

Members or other parties, unless those parties are performing work on Merit's behalf.

This policy does not apply to networks, host computers, other equipment, or systems that are managed by Merit on behalf of another party. In such cases the labeling, banners, domain names assigned, and other written information should make it clear who is responsible for privacy policy decisions related to information collected and stored on these networks, host computers, and systems. Parties for whom Merit manages networks, host computers, other equipment, or systems are encouraged to develop and post their own privacy policies. When no such specific privacy policy exists, Merit will follow the rules and procedures given in this policy; however, the parties for whom Merit manages the networks, host computers, other equipment, or systems are not governed or bound by Merit's Privacy Policy.

Sensitive, Confidential, or Personally Identifiable Information

For the purposes of this policy, confidential information is information that Merit will not reveal to third parties or will only reveal to third parties under conditions outlined in this policy. The expectation of confidentiality may arise from a written non-disclosure agreement, contract, or other agreement with Merit, or through requirements imposed by laws or regulations. The Merit Acceptable Use Policy and this Privacy Policy establish an expectation of confidentiality as well as bounds for that expectation between Merit and its Members and other users of Merit's facilities, products, and services.

Sensitive information is information for which it is not possible to determine if the information should be considered confidential without additional context. Such additional contextual information may be available to the individuals or organizations that send or receive the information, but is usually not available to Merit. Sensitive information is also information that may not be confidential by itself, but which may become confidential when found or used in a particular context or when combined with other information. For example, the amount of data sent or received by a single site attached to Merit is not considered confidential, but the amount of data sent or received between two sites is considered confidential. Because sensitive information may be confidential, Merit gives sensitive information a very high degree of privacy protection and will not release this information to third parties except as allowed by the Merit Acceptable Use Policy and this Privacy Policy.

Personally identifiable information is information that could be used directly or indirectly to identify the individual who is the subject of the information. Information is personally identifiable if a recipient of the information could use the information alone, or in combination with other information, to identify an individual. Without specific evidence to the contrary, information that includes one or more of the following items must always be considered personally identifiable: name; address, including street address, city, county, zip code, or equivalent geocodes; names of relatives and employers; birth date; telephone and fax numbers; e-mail addresses; social security number; other identification numbers such as medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; any vehicle or other device serial numbers; web URL; Internet Protocol (IP), ethernet, and other network media addresses; Internet domain names; finger or voice prints; photographic images; and any other unique identifying numbers, characteristics, or codes (whether generally available in the public realm or not) that may be available to recipients of the information. Merit gives personally identifiable information a very high degree of privacy protection and will not release this information to third parties except as allowed by the Merit Acceptable Use Policy and this Privacy Policy.

What Information Is and Is Not Collected, How It Is Used, and How Long It Is Kept

Merit automatically gathers certain information about the usage of or access to Merit's networks, Web sites, Web caches, File Transfer (FTP) sites, Network News and other servers. For example the information gathered may include the number and frequency of visitors to a site, the links that referred a user to a site, the pages and files accessed, the type of browser used, the screen resolution, or the amount of traffic sent and received over segments of the networks Merit operates. Merit only uses and keeps such data in the aggregate, but may hold more detailed information for brief periods of time while the aggregate reports are being produced. This aggregate data is not considered to be confidential and is kept indefinitely. This aggregate data helps Merit determine how its sites, networks, and services are used, so Merit can improve its sites, networks,

and services or make projections of future growth. In some cases, the information gathered may be used to bill a Member or to establish the rate that a Member should pay.

Merit collects information about each Merit shared dial-in session, including the AccessID used to authorize the dial-in session, the name of the Network Access Server (NAS) and port that answered the call, the phone number called (not always available), the phone number that originated the call (not always available), the IP address assigned to the dial-in session, the date and time when the dial-in session started, its duration, and the total number of packets and bytes sent and received during the session. This information is kept indefinitely. The collected information is used to produce aggregate network usage reports, to support billings for surcharged network services, to investigate and troubleshoot the operation of the dial-in network, to investigate complaints about possible network abuse and violations of the Merit Acceptable Use Policy, and occasionally to respond to warrants, subpoenas and other court orders. Merit does not collect information about what was done or what sites were visited during the dial-in session.

Merit collects information about uses or logins to certain host computers operated by Merit, including the Login ID used to authorize the session, the name of the host computer being accessed, the IP address used for access to the host computer, the date and time when a session started, its duration, and the total number of packets and bytes sent and received during the session. This information is kept indefinitely. The collected information is used to produce aggregate network usage reports, to support billings for network services, to investigate and troubleshoot the operation of the host computer or the networks to which the host computer is attached, to investigate complaints about possible network abuse and violations of the Merit Acceptable Use Policy, and occasionally to respond to warrants, subpoenas and other court orders. Merit does not collect detailed information about what was done during a session.

Merit may specifically ask for or receive information about individuals when they sign up to use a particular service, participate in an on-line e-mail list, forum or course, provide information via a Web form or similar input process at a Web site, attend a conference or other event, ask a question, or request information. In these cases Merit needs the information -- such as an individual's name or other identifier, e-mail address, history of course or learning experience, billing address, or credit card number -- in order to provide the requested service. The length of time that such data is kept will vary depending on the purpose for which it was gathered.

Merit may collect or examine information carried in the user data portion of network packets when troubleshooting certain types of network malfunctions, when investigating possible violations of the Merit Acceptable Use Policy, or occasionally as required by law, but Merit does not routinely collect or examine this information.

Merit may collect or examine information such as the source and destination IP addresses carried in the headers of network packets when troubleshooting certain types of network malfunctions, when investigating possible violations of the Merit Acceptable Use Policy, or occasionally as required by law, but other than the aggregate statistical information described earlier, Merit does not routinely collect this information.

Merit Members may request assistance from Merit in troubleshooting certain types of network malfunctions or in investigating possible violations of the Merit Acceptable Use Policy or the Member's own policies. With the advance written approval of an official representative of the Member, Merit may elect to collect sensitive, confidential, or personally identifiable information. All of the information to be collected must be related to the use of networks, hosts, or other systems that belong to or involve products or services provided by Merit to the Member.

Sensitive, confidential, or personally identifiable information collected when troubleshooting network malfunctions is kept only as long as necessary to resolve the problem. Sensitive, confidential, or personally identifiable information collected when investigating possible violations of the Merit Acceptable Use Policy are kept until the investigation is complete and may be kept indefinitely when it shows actual violations of the Merit Acceptable Use Policy.

Merit does not gather information about the sites visited by individuals or the detailed network usage patterns of individuals or organizations, other than the aggregate statistical information and information about visits to sites and services operated by Merit described earlier.

Merit web sites may use cookies to preserve user information between web pages in order to provide a usable user interface. Merit web sites may use cookies to restore user-selected preferences at future visits. Merit web sites will not attempt to read any non-Merit session cookies stored on a user's computer.

A user may decline to use cookies and will still be able to access most parts of Merit web sites. Portions of the Merit web site that require authentication will not be available if cookies are disabled.

Disclosure

Merit never sells, lends, or leases sensitive, confidential, or personally identifiable information to third parties.

Merit will not share or disclose sensitive, confidential, or personally identifiable information to third parties unless required to do so by law or when in Merit's judgment release is required to prevent serious injury or harm that could result from violation of the Merit Acceptable Use Policy. Unless prohibited by law or in cases of extreme emergency where any delay in releasing information will increase the risk of serious injury or harm, Merit will inform and consult with the official representatives of the Members involved in writing before releasing sensitive, confidential, or personally identifiable information to third parties. An extreme emergency is a situation where attempts to contact the Member involved have been unsuccessful and any further delay in providing information to a third party is very likely to result in serious injury, death, or other similar, serious harm to individuals.

When disclosure is required by law, Merit will allow the Member involved to participate in discussions with and make arguments to the court or agency requiring disclosure when such participation is permitted by the court, agency, or relevant law. Unless prohibited by law, when Merit is not able to inform and consult with the Members involved before releasing sensitive, confidential, or personally identifiable information to third parties, Merit will inform the Members involved as soon as possible after the fact.

Merit may elect to share sensitive, confidential, or personally identifiable information with the official representatives of its Members, but only when all of the information to be shared relates to use of networks, hosts, or other systems that belong to or involve products or services provided by Merit to the Member.

Merit may elect to share aggregate statistical information that is based on or derived from sensitive, confidential, or personally identifiable information so long as the aggregate information when used alone or when combined with other information is no longer confidential or sensitive and will not reveal the activities of or information about individuals or detailed information about organizations.

Merit may elect to engage in collaborative research projects that use sensitive, confidential, personally identifiable, or aggregate statistical information subject to the safeguards outlined below. Such use will always be limited to the minimum information necessary to meet the needs of the research project and Merit staff will maintain control over any sensitive, confidential, or personally identifiable information used.

Some personally identifiable information that individuals or organizations furnish to Merit may be disclosed as a normal part of the use of that information. For example, the names and e-mail addresses of individuals subscribed to some of the public e-mail lists that Merit operates are available to the public or to other list subscribers or become known to list subscribers when messages are posted to the list, or the name and work phone number of an official representative of Merit's Members may be shared with third parties seeking assistance or reporting problems.

Safeguards

Merit strives to operate its networks, host computers, and other systems in a professional and secure manner and to do business with other organizations that do the same.

Staff are made aware of this policy and the Merit Acceptable Use Policy when they are hired. Staff are reminded of both policies periodically. Staff who violate this policy or the Merit Acceptable Use Policy are subject to disciplinary action up to and including dismissal. Merit and the individual(s) involved may also be subject to sanctions and penalties as provided by law.

Access to sensitive, confidential, or personally identifiable information is limited to staff with a need to access or use the data. Appropriate security, including physical security, is in place to prevent inappropriate or accidental access or release. When appropriate, stored data may be encrypted to provide additional protection. Care is taken that information is not inadvertently kept for much longer periods than intended as part of automatic disk or other backup procedures.

Staff engaged in troubleshooting and repairing networks, host computers, or other facilities and services may occasionally find it necessary to or may inadvertently gain access to or view small amounts of sensitive, confidential, or personally identifiable information. Any more extensive, routine, or long term logging or monitoring of sensitive, confidential, or personally identifiable information required for troubleshooting or repair must be approved in writing in advance by Merit management. An official representative of the Member involved will be informed in writing when such logging or monitoring is taking place.

All disclosures of sensitive, confidential, or personally identifiable information to third parties require the approval of at least two staff members, one of whom must be a Director at Merit or Merit's President. Exceptions to this provision can only be made in cases of extreme emergency when attempts to contact senior Merit management have failed and further delay is likely to result in serious injury or harm as outlined above.

Merit limits the amount of sensitive, confidential, or personally identifiable information that it keeps as well as the length of time that such data is kept. When IP addresses or domain names that are or could become personally identifiable when combined with other information must be kept for longer periods of time, Merit anonymizes the information that is kept so that the information is still useful for statistical and other forms of analysis, but it can no longer be used to identify the activities of individuals.

When sensitive, confidential, or personally identifiable information is used as part of a research project, the project must be reviewed and approved by the relevant Human Subjects Institutional Review Board (IRB) or there must be a written statement from the IRB stating that the project is exempt from further IRB review.

When sensitive, confidential, or personally identifiable information is used as part of a research project that includes researchers from organizations other than Merit, there is a written agreement between the research project and Merit that specifies in detail how the information may and may not be used, and how it will be protected. Agreements will be tailored to the needs of individual projects, but would typically include requirements that researchers:

- limit use of the information to the specific purposes of the research project,
- limit use to packet header information only,
- allow no use of the user data portion of any network packets,
- restrict access to the information to only those individuals that are part of the research project and who have been made aware of the agreement and the sensitive nature of the data,

- safeguard the data to prevent its inadvertent disclosure,
- anonymize all data that will be kept for more than a specified period of time (from a few hours to several days, but not weeks or months) by discarding the user data portion of the packets and at least the last eight bits of all IP addresses and preferably all of the bits in the non-network portion of an address that are not on a list of IP addresses that has been reviewed and approved by Merit as posing no risk of identifying the actions of individuals as soon as is practical (within a few hours to a few days),
- keep data that has not been anonymized including copies of data made as part of disk or other backup procedures only as long as necessary (generally no longer than a few days without specific written permission from Merit),
- return or destroy all sensitive data at the conclusion of the research project,
- limit formal and informal publication of the research results so that the activities of specific individuals or organizations are not disclosed,
- warrant that all required IRB approvals have been obtained, or will be obtained before any personally identifiable information is used and that all required IRB approvals will be maintained and renewed as necessary or access to and use of personally identifiable information will cease,
- allow Merit staff to review information that is to be published in advance to ensure that this agreement has been followed, and
- acknowledge that the information remains Merit's property, that only Merit may authorize additional access to or release of the information, and that all requests for access to or disclosure of the information will be immediately forwarded to Merit.

Disclosure as Required or Prohibited by Law

Through warrants or other court orders, subpoenas, or other requirements of law, Merit may be required to gather and/or release information including sensitive, confidential, or personally identifiable information that would otherwise not be subject to release under the Merit Acceptable Use Policy or this Privacy Policy. When Merit receives such requests to release information, an official representative of the Member involved will be notified of the request and given an opportunity to contest the release of information when such notification is not prohibited by the warrant, order, or subpoena. When such advance notification is prohibited, Merit will notify an official representative of the Member of the release of information as soon as such notification is allowed.

A number of laws prohibit Merit from gathering or releasing certain types of information or specify the conditions that must exist and the procedures that must be followed when certain types of information are gathered or released. Laws and regulations also provide privacy protection to and impose privacy protection requirements on individuals and organizations for certain types of information. Merit will itself follow the requirements imposed by law and regulation and will to the greatest extent allowed or required by law or regulation give an official representative of the Member involved advance notice of and an opportunity to be heard on any request for release of information as described above.

The federal, state, and other laws and regulations that govern the release of information are complex and it is not possible to outline all of the considerations that might apply without reference to a particular context and set of facts. However, some of the laws and regulations that are most likely to apply to electronic communication over Merit's network are listed below:

- Wire And Electronic Communications Interception And Interception Of Oral Communications, U.S. Code Title 18, Chapter 119, which states in part:

Sec. 2511(3) ... a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

- Electronic Communications Privacy Act (ECPA), U.S. Code Title 18, Chapter 121 - Stored Wire And Electronic Communications And Transactional Records Access, which states in part:

  Sec. 2702(a) (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service ....

- Family Educational Right to Privacy Act (FERPA), U.S. Code Title 20, Chapter 31, Part 4, Sec. 1232(g), which governs "... the release of education records (or personally identifiable information contained therein other than directory information, ...) of students without the written consent of their parents ...."

- Michigan's Library Privacy Act, MCL 397.601-606, which exempts library records from disclosure under Michigan's Freedom of Information Act (FOIA) and also states in part:

  Sec. 3(2): Unless ordered by a court after giving the affected library notice of the request and an opportunity to be heard on the request, a library or an employee or agent of a library shall not release or disclose a library record or portion of a library record to a person without the written consent of the person liable for payment for or return of the materials identified in that library record.

- Michigan's Freedom of Information Act (FOIA), MCL 15.231-246, which sets requirements for the disclosure of public records by all "public bodies" in Michigan. Exempt from disclosure under section 13(1) of the Act is:

  (a) Information of a personal nature where the public disclosure of the information would constitute a clearly unwarranted invasion of an individual's privacy,

  and

  (d) Records or information specifically described and exempted from disclosure by statute.

Responsibilities of Others

Because the networks, host computers and other systems managed and controlled by Merit are only some of the networks, host computers, or systems that will carry a user's or organization's data when they use the Internet, the privacy of sensitive, confidential, or personally identifiable information is often beyond Merit's control. In the final analysis Members must understand that they and their users assume substantial responsibility for the security of their information.

Merit strongly urges that particular care be taken to protect any passwords that are used. Passwords should not be divulged to anyone. Members should caution users to always log out of browsers or other online applications at the end of each computer session to ensure that others cannot access their personal information and correspondence, especially if they share a computer with someone else or are using a computer in a public place like a library, school computer laboratory, or Internet cafe. The use of network applications such as ssh and PGP that encrypt data that is sent over the network should be considered and is encouraged.

Members should instruct users that when communicating with others online and disclosing personal information such as their actual name, e-mail address, on a web page, in a newsgroup, chat room, forum, or in an e-mail message, that information may be collected and used by others in ways that they did not intend or approve. Care should always be exercised when disclosing confidential, sensitive, or personal information either electronically or by more traditional means.

Changes to this Policy

Any changes to this policy or the Merit Acceptable Use Policy must be approved by the Merit Board of Directors. If either policy is changed, Merit will post the revised policy on its Web site (www.merit.edu) and elsewhere. Because these policies may be updated from time to time, it is the responsibility of the Member or user to check and review the policies periodically.