# NON-EMPLOYEE CONTINGENT WORKER ACKNOWLEDGMENT

You (hereinafter referred to as "You", "Your", "Yourself" or "Non-Employee") have been engaged or assigned to work at Regeneron by your employer or service provider to supply services to Regeneron Pharmaceuticals, Inc., and/or one of its affiliates (collectively referred to as "Regeneron") in accordance with terms and conditions under an agreement between Your employer or service provider and Regeneron ("Agreement") under which You will be providing services subject to such Agreement. As part of your assignment, Regeneron may disclose certain Regeneron Confidential Information to You (as defined below). Further, due to the performance of services by You on Regeneron's premises and otherwise on Regeneron's behalf, You will likely interact with Regeneron employees and have access to Regeneron equipment and systems. In light of the Agreement and its obligations and in consideration of Regeneron accepting Your assignment, You agree to follow the instructions of Your employer or service provider and You agree to the following terms of this Acknowledgement:

## 1. You Must Not Use or Disclose Regeneron Confidential Information.

1.1 "Confidential Information", whether in written, electronic, oral, visual, or tangible form, means any trade secrets or confidential information relating or belonging to Regeneron including but not limited to any such information relating to Regeneron's materials, reagents, procedures, research and development programs, data, information, results, conclusions, experience, business and marketing strategies and plans, formulae, products, processes, procedures, methods, results, reports, documents or know-how, whether technical or non-technical, customers, customer lists or requirements, price lists or pricing structures, sales specifications and information, business plans or dealings or developments, employees or officers, financial information and budgets, designs, formulae, product lines, research activities, corporate image strategy or dealings, legal affairs, services, computer source codes, software, prototypes, past or proposed business dealings or transactions, any document marked 'Confidential', (or with a similar expression), or any information which the Non-Employee has been told is confidential or which the Non-Employee might reasonably expect Regeneron would regard as confidential, or any information which has been given to Regeneron in confidence by distributors, suppliers and other persons.

1.2 Non-Employee agrees to hold Confidential Information in confidence. Non-Employee shall not, either during the assignment or after its cessation, whether directly or indirectly (i) disclose Confidential Information to anyone, or (ii) use Confidential Information for any purpose other than to provide services in accordance with the Agreement. The Non-Employee shall not at any time during the assignment make any notes or memoranda relating to any matter within the scope of Regeneron's business, dealings or affairs otherwise than for the benefit of Regeneron.

1.3 The obligations and restrictions in clause 1 shall not apply to the extent that (i) the information was public knowledge at the time of such disclosure other than as a result of unauthorised disclosure; (ii) the Non-Employee disclosed the Confidential Information in good faith to report an offence to a law enforcement agency or regulatory body; or to co-operate in good faith with a criminal investigation or prosecution. Nothing in this Acknowledgment shall be construed to prohibit or otherwise restrict Non-Employee from lawfully reporting waste, fraud, or abuse to a designated investigative or law enforcement representative of a United States federal department or agency or other governmental authority authorized to receive such information under an applicable U.S. Government procurement law or other applicable law.

**2. Return of Confidential Information.**

2.1 Upon the written request of Regeneron, or at the cessation of Your assignment (whichever is earlier) Non-Employee shall destroy or return (as directed by Regeneron) all Regeneron Confidential Information, including passwords, whether in written or electronic form, and any drafts, copies, summaries, and extracts, of Confidential Information (including derivative analysis based on the Confidential Information). At Regeneron's request, Non-Employee shall assist in the migration of Confidential Information to Regeneron or any third party identified by Regeneron.

**3. Intellectual Property.**

3.1 You understand that the Agreement governs ownership rights generally between Regeneron and Your employer or service provider and You regarding your performance of services to Regeneron, such as to any materials, knowledge, deliverables, and products developed as well as any existing and new intellectual property rights. You shall, prior to commencement of your assignment, enter into an agreement with Your employer or service provider regarding intellectual property rights related to the assignment.

3.2 For the avoidance of doubt, you agree that Regeneron is the sole and exclusive owner of any data, information, reports, designs, names, software, code, string identifiers, uniform resource locators, metadata, processes, presentations, materials, and all intellectual property rights (including all inventions, discoveries, improvements, know-how, copyrights, trademarks and associated good will) generated or developed during the assignment (collectively, "Deliverables") as well as any Regeneron Confidential Information.

3.3 By way of further explanation, You agree to assign and hereby assign all right, title, and interest in and to the Deliverables to Regeneron. In the event that any Deliverable does not legally qualify as a work made for hire under copyright law, You shall assign, and hereby assign, all right, title, and interest in and to such Deliverable to Regeneron or its nominee without further compensation from Regeneron. In the event that an assignment of the copyrightable material is not possible, You agree to, and hereby do, grant Regeneron an exclusive (even as to You), sublicensable, perpetual, irrevocable, transferable, royalty-free, fully paid-up, worldwide license in all rights to said copyrightable material for the entire duration of any such copyright (including any extensions of such copyright available now or in the future). Regeneron shall have the exclusive right to copy, publish, perform, use, exploit, advertise, and exhibit all Deliverables and to authorize others to do so for any lawful purpose as Regeneron in its sole discretion shall determine. Whenever requested to do so, You shall execute any and all documents and give testimony that Regeneron deems necessary to apply for and obtain trademarks, domain names, copyrights, letters patent of the United States, United Kingdom, Ireland or of any foreign country or to protect otherwise Regeneron interests therein.

**4. Independent from Regeneron.**

4.1 Your status as Non-Employee is that of an individual who has been engaged or assigned to work at Regeneron by your employer or service provider to supply services to Regeneron and not that of an agent or employee of Regeneron and, as such, You agree that You shall not have the right or power to enter into any contracts, agreements, or any other commitments on behalf of Regeneron. You expressly acknowledge that You

are not an employee of Regeneron and You are not entitled to participate in any benefit plans of Regeneron. You understand that Your engagement with Regeneron will not result in a guarantee, promise or expectation of employment with Regeneron. You further agree not to hold Yourself out to third parties as an employee or officer or agent of Regeneron.

4.2 Nothing in this Acknowledgement shall affect or diminish the continuing applicability of similar obligations imposed upon the Non-Employee in Your contract of employment or engagement with your employer or service provider.

**5. Regeneron Policies and Procedures.**

5.1 You understand that while on Regeneron premises, or otherwise while performing services on behalf of Regeneron, You must follow commercial standards of professional behavior and certain mandatory policies applicable at the Regeneron workplace. While You are not a Regeneron employee, You must abide by the workplace policies and procedures of Regeneron during Your time performing services for Regeneron, including those attached to this Acknowledgement as Exhibit A.

**NON-EMPLOYEE**

By: _____
Signature

Name: _____
Print

Date:_____

EXHIBIT A – see attached Regeneron Policies

# DEBARMENT CERTIFICATION FOR CONTINGENT WORKERS

As you know, Regeneron is committed to doing the right thing and to complying with the laws and regulations that govern our conduct. In connection with those obligations, we need individuals to be aware of certain regulations relating to what is known as "debarment," which is the process by which the US Food and Drug Administration (FDA) excludes certain persons from submitting, or assisting in the submission of, any regulatory application. Section 306(a)(2)(B) of the Food, Drug and Cosmetic Act (21 U.S.C. 335a(a)(2)(B)) requires debarment of an individual if the FDA finds that the individual has been convicted of a felony under Federal law for conduct relating to the regulation of any drug product. Felonies include submitting false data to the FDA, lying to FDA investigators, paying or accepting bribes, and selling prescription drug samples.

Regeneron is required under Section 306(k) of the Food, Drug, and Cosmetic Act to certify that Regeneron has not and will not use in any capacity the services of any debarred persons in connection with our drug product applications to the FDA.

By signing, you certify you are not debarred or in the process of being debarred by the FDA or any foreign equivalent authorities. You are also certifying that you are not excluded from any federal health care program or disqualified by any federal or state law. You also are agreeing to inform Regeneron if in the future you are notified of debarment/exclusion proceedings or become debarred/excluded. Please contact your Regeneron business contact in writing immediately.

***Certification***

***I certify that I am not debarred by the FDA under 21 U.S.C. § 335a or any foreign equivalent I am not threatened with debarment by a pending proceeding, action, or investigation. I am also certifying that I am not excluded from participating in any federal health care program under 42 C.F.R. Part 1001 et seq., or am the subject of an exclusion proceeding, or am otherwise disqualified under federal or state law, or to my knowledge am threatened with such disqualification by a pending proceeding, action, or investigation. I certify I will immediately notify Regeneron in writing if any such debarment, exclusion, or disqualification occurs, or if any such debarment, exclusion, or disqualification, proceeding, action, or investigation is commenced.***

Name (printed): _____

Signature:_____

Date:_____

If you have questions regarding your ability to certify that you are not debarred or disqualified, or not in the process of debarment or disqualification, please contact your Regeneron business contact.

Please refer to the FDA Debarment list to check if you are debarred.

Please refer to the FDA notice of Opportunity for Hearing (NOOH) – Proposal to Debar to check if you are in the process of debarment.

REGENERON
SCIENCE TO MEDICINE®

**POLICY NAME:**
# 123 Anti-Harassment

**Effective Date: 01/01/01**
**Revised Date: 10/08/18**
**Contact: HRBPBUSINESSPARTNERS@REGENERON.COM**

## PURPOSE

Regeneron is committed to providing a work environment that is free from all forms of discrimination and unlawful harassment.

## SCOPE

This policy applies to all employees of Regeneron, its subsidiaries, and all locations where employees are working for or representing Regeneron or attending Regeneron-sponsored events.

## POLICY

Regeneron has a policy of zero-tolerance with respect to sexual and other employee harassment that is unlawful under federal, state, and local law. Regeneron expressly prohibits any form of sexual or otherwise unlawful employee harassment including, but not limited to, actions, words, jokes, or comments based on an individual's race, color, religion, sex, national origin, age, citizenship status, sexual orientation, disability, genetic information, familial status, gender identity, military or veteran status or any other protected characteristic in accordance with applicable federal, state and local law. Regeneron provides ongoing anti-harassment training to ensure employees can work in an environment free of sexual or other unlawful employee harassment.

Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, and other visual, verbal or physical conduct (including online conduct) of a sexual nature when this conduct explicitly or implicitly affects an individual's employment, unreasonably interferes with an individual's work performance, or creates an intimidating, hostile, or offensive work environment. This definition includes many forms of offensive behavior and includes gender-based harassment of a person of the same sex as the harasser. Sexual harassment can occur between any individuals, regardless of their positions at the Company. Examples of offensive conduct expressly prohibited by this policy include, but are not limited to:

- threatening or insinuating, expressly or implicitly, that a subordinate is required to submit to sexual advances or to provide sexual favors as a condition of employment, continued employment or any term, condition or benefit of employment, or that a subordinate's refusal to submit to sexual advances or to provide sexual favors will adversely affect the subordinate's evaluation, employment, continued employment or any term, or condition or benefit of employment;

- making any employment decisions or taking any employment action based on a person's submission to or refusal to submit to sexual advances;
- engaging in unwelcome sexually-oriented conduct which has the purpose or effect of interfering with another person's work performance or of creating an intimidating, hostile, abusive, or offensive work environment.
- requests or demands for sexual favors;
- repeated and unwelcome requests for dates;
- unwelcome physical contact, such as patting, pinching, or brushing against another person's body;
- sexual bantering, "jokes", and "teasing";
- sexual, suggestive, or biased jokes;
- sexual flirtations, advances, or propositions;
- verbal abuse of a sexual nature;
- verbal commentaries about an individual's body, sexuality, or sexual orientation;
- sexually degrading words used to describe an individual; discussions of or questions about sexual desires, sexual fantasies, sexual frustrations, etc.;
- sexually-explicit or sexually-suggestive objects, cartoons, software, photos, or pictures in the workplace;
- sexually-oriented or degrading gestures;
- verbal or nonverbal innuendo of a sexual, suggestive, or biased nature;
- other nonverbal communications of a sexual or suggestive nature, such as leers and gawks;
- obscene, off-color, or otherwise hostile language of a sexual, suggestive or biased nature;
- offensive e-mail, voicemail messages, textmessages, or other messages sent via electronic equipment, regardless of whether such equipment was provided by the Company;
- offensive posts on social media sites;
- any other behavior of a hostile or abusive nature directed at one sex, even if not sexual in nature; and
- any other inappropriate behavior of the kind or similar to that referred to elsewhere in this policy.

It is no defense to inappropriate behavior that there was no bad intent, that it was only a joke, or that it was not directed at any particular person.

The prohibitions on inappropriate behavior set forth above apply not only to the workplace itself, but also to all other work-related settings, such as business trips and business related social functions. These prohibitions also apply in connection with electronic or other online interactions between or amongst Company employees.

## COMPLAINT PROCEDURE

It is the responsibility of each Regeneron employee and all members of Regeneron management to create an atmosphere free of harassment, sexual or otherwise. In addition, it is the responsibility of each employee to respect the rights of his or her coworkers.

It is the responsibility of Regeneron employees who experience any job-related harassment to use this Complaint Procedure, which has been established for the purposes of preventing and correcting

unacceptable workplace behavior. If an employee experiences or witnesses sexual or other unlawful harassment in the workplace, discrimination and/or retaliation, he or she should report it immediately to his/her immediate supervisor.

If, for some reason, the employee does not feel comfortable reporting the incident of harassment, discrimination or retaliation to his/her immediate supervisor, he or she should immediately report it to:

- the Human Resources Department
- the Law Department or
- any other member of management

If the employee is uncomfortable speaking to a supervisor, the following are ways to make an anonymous report:

- Call the Compliance Hotline at: 1-877-RGN-ETHX (1-877-746-3849)
- Post an anonymous on-line report at https://www.ethicspoint.com/ (select “File a Report”)

Please be advised nothing in this policy prohibits employees from directly confronting the alleged harasser and asking him or her to stop the offending behavior. However, this policy does not require any employee to do so.

**Employees can raise concerns, make reports, and participate in the investigation of other employees’ claims without fear of reprisal or retaliation.**

Any supervisor or manager who becomes aware of possible sexual or other unlawful harassment must immediately advise the Human Resources Department or the Law Department so it can be investigated in a timely manner. A supervisor or manager who fails to report sexual harassment, or otherwise knowingly allows it to continue, will be subject to discipline, up to and including termination of employment.

All allegations of sexual harassment or other unlawful workplace harassment will be promptly and thoroughly investigated in a timely manner. Regeneron takes such allegations seriously and will carry out a fair investigation, taking into account facts, circumstances, and information from all parties. The investigation may include, for example, the collection of documents or witness interviews. To the extent possible and appropriate, the employee's confidentiality and that of any witnesses and the alleged harasser will be protected against unnecessary disclosure, and information shall be provided to others on a need-to-know basis only.

Each circumstance will be evaluated for appropriate corrective action. Anyone engaging in sexual or other unlawful harassment, discrimination and/or retaliation will be subject to disciplinary action, up to and including termination of employment. Even if conduct does not constitute discrimination, harassment, or retaliation in the legal sense, an employee, manager, supervisor, or agent who engages in inappropriate behavior inconsistent with this policy will be subject to discipline, up to and including termination of his or her employment or other relationship with the Company.

**NO RETALIATION**

Regeneron expressly prohibits any form of retaliatory action against any employee availing him/herself of the benefits of this procedure, or assisting or testifying in any investigation or proceeding involving a complaint.

However, if after investigating any complaint of harassment or unlawful discrimination or retaliation, Regeneron determines the complaint was made in bad faith or with malicious intent, or an employee has provided false information regarding the complaint, disciplinary action, up to and including termination of employment, may be taken against the individual who filed the complaint or gave the false information.

**New York Addendum: External Resources**

In addition to Regeneron's Complaint Procedure, employees have the right to file a complaint with government agencies, such as those listed below, alleging violations of federal anti-discrimination laws, such as Title VII of the Civil Rights Act of 1964, or the New York State Human Rights Law. Employees can also pursue a civil claim in the courts.

Office of the NYS Attorney General Civil Rights Bureau
28 Liberty Street, 15th Floor, New York, NY 10005
civil.rights@ag.ny.gov

U.S. Equal Employment Opportunity Commission
http://www.eeoc.gov
info@eeoc.gov

NYS Division of Human Rights
One Fordham Plaza, Fourth Floor, Bronx, New York 10458
http://www.dhr.ny.gov

NYC Commission on Human Rights
40 Rector Street, 10th Floor, New York, New York 10006
http://www.nyc.gov/html/cchr

There may be additional local laws and agencies depending where an employee works.

The federal, state, and local agencies may have the power to award relief, which varies on a case-by-base basis, but may include requiring an employer to take action to stop discrimination or harassment, or to redress damage caused, including monetary damages, attorneys' fees, and civil fines. State or federal courts may also award remedies if they determine that discrimination has occurred.

REGENERON
SCIENCE TO MEDICINE®

**POLICY NAME:**

# 520 Information Security: Acceptable Use of Business Information and Information Systems

**Effective Date:**
**Revised Date: 01/29/18**
**Contact: ITCOMMUNICATIONS@REGENERON.COM**

## PURPOSE

This policy defines the guiding principles that all Regeneron personnel and other authorized users (such as contractors and business partners) will use when accessing Regeneron assets, systems or data. This policy ensures usage of Regeneron IT components is done in a standard and approved manner across the enterprise.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), data loss or theft, lost productivity resulting from network downtime, and loss related to legal or regulatory violations (criminal and/or civil).

Everyone who works at Regeneron is responsible for the security of our information systems (internal & external) and the data that resides on or passes through them. Consequently, all employees must ensure they adhere to the guidelines in this policy at all times. Anyone who is unclear on the policy or how it impacts their role should speak to their manager or contact Regeneron Information Security.

Business Information and Information Systems are strategic assets of Regeneron and must be treated and managed as valuable resources. Regeneron provides various computer resources to its employees and contractors for the purpose of assisting them in the performance of their job-related duties.

Violations of this policy can result in discipline up to and including termination of employment.

## SCOPE

This policy applies to all personnel who access Regeneron systems or data. Components covered by this policy may include: Data Management, Identity & Authentication Credentials (e.g., user IDs and passwords), and Computing Systems (cloud, server, workstation, & mobile).

For some users and/or some systems, a more specific policy may exist. In such cases, the more specific policy has precedence in areas where they conflict, but otherwise both policies apply.

Some aspects of this policy may affect areas governed by local legislation in certain countries (e.g., employee privacy laws). In such cases, the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases, local teams should develop and issue users a clarification of how the policy applies locally.

Staff members at Regeneron who monitor and enforce compliance with this policy are responsible for ensuring they remain compliant with relevant local legislation at all times.

## POLICY

**Policy Objectives:**

This Acceptable Use Policy is established to achieve the following:

- Protect Regeneron, our employees, customers, and other partners from harm caused by the misuse of our IT systems and our data. (Misuse includes both deliberate and inadvertent actions.)
- Establish appropriate and acceptable practices regarding the use of information resources.
- Ensure compliance with applicable law and other rules and regulations regarding the management of information resources.
- Educate individuals who may use information resources with respect to their responsibilities associated with computer resource use.

1.1 General

The policy statements in this section are a reminder that the way employees use company resources can affect the reputation of Regeneron, and may have legal implications.

1.1.1 All users are required to review this policy at the time they are granted systems access, as well as annually. For reference, this and other security policies, as well as the Employee Handbook may be found on RON.

1.1.2 Users shall not engage in any illegal activity according to local, state or federal law, including theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations, (e.g., HIPAA or SOX).

1.1.3 Users shall not engage in any activities that are inappropriate for Regeneron to be associated with or are detrimental to Regeneron's reputation: This includes sending or viewing pornography, racist, or otherwise offensive materials; any activity violating Regeneron's anti-harassment policies, work rules, or any other Regeneron policy; or activities that intentionally access, create, store or transmit material which Regeneron may deem to be offensive, obscene, or contradictory to any company policy.

1.2 Monitoring

The monitoring and blocking done by Regeneron Information Security serves as a layer of defense against scammers, cyber-criminals, and other malicious actors; and provides an audit-trail in the event of an incident or cyber-attack.

1.2.1 Appropriate Regeneron personnel (Human Resources, Information Security, Law Department, and Corporate Compliance) may, with appropriate approvals, monitor

the use of any of its systems or data at any time, for any reason; and act, within the limits of applicable laws, upon any information learned from this monitoring. This may include examination of the content stored within the email and data files of any user, and examination of the access history of any user. Accordingly, Users should have no expectation of privacy regarding the information transmitted through or stored on Information systems.

1.2.2 Regeneron may regularly audit networks and systems to ensure compliance with this policy.

1.3 Regeneron's Security Controls

There are a variety of technical security controls in place throughout the network and on end-user devices. The purpose of these controls is to safeguard Regeneron's systems and data.

1.3.1 Users shall not attempt to circumvent any protections on a Regeneron-owned Computing System, including attempting to access any data, documents, email correspondence, and programs contained on Regeneron systems for which they do not have authorization.

1.3.2 Users shall not engage in activity (including the use of tactics, hardware, or software) that may degrade the performance of information resources; deprive an authorized user access to Regeneron resources; obtain extra resources beyond those allocated; or attempt to evade or circumvent Regeneron's protective controls, policies, or processes.

1.3.3 Users shall not download, install or run security programs or utilities such as password cracking programs, packet sniffers, encryption tools, or port scanners that can reveal or exploit weaknesses in the security of a Regeneron computer resource.

1.4 Physical Security

Regeneron issues physical devices such as laptops, phones, and tablets to end users. In addition, users may also possess hardcopy printouts that contain company data. The policy statements in this section serve as guidelines to help prevent the unintentional loss of devices and the data they contain or have access to.

1.4.1 Users shall take reasonable efforts to ensure the security of portable devices in public spaces; the use of cable locks and other physical security mechanisms is encouraged when operating outside of a Regeneron corporate location.

1.4.2 Users shall not leave portable computing devices unattended in public places, e.g. airports, conference centers, hotel lobbies, etc.

1.4.3 Users shall secure portable devices to the greatest extent possible prior to leaving them in unattended vehicles, e.g., placing them inside the trunk when one is available.

1.4.4 Users shall report the loss, theft, or compromise of any Regeneron asset, system or data (including printed material) to their supervisor and/or to the IT Call Center.

1.4.5 Users shall ensure that visitors, vendors, or external parties brought in to Regeneron facilities adhere to this policy.

1.5 Incidental Use

Regeneron allows incidental use of its systems for personal purposes. These policy statements help to protect Regeneron's systems and data and serve as guidelines for personal use of company-owned systems.

1.5.1 Regeneron's systems exist to support and enable Regeneron business activities. However, incidental personal use is allowed. Incidental use shall not be in any way detrimental to Regeneron, or to a user's productivity or that of their colleagues; nor should it result in any direct costs being borne by Regeneron other than for trivial amounts (e.g., occasional short telephone calls).

1.5.2 Regeneron trusts users to be fair and sensible when judging what constitutes an acceptable level of incidental personal use of the company's IT systems. If users are uncertain, they should consult their manager or Regeneron Information Security.

1.5.3 Regeneron Information Security Management will resolve incidental use questions and issues using these guidelines in collaboration with Regeneron HR and Legal.

1.5.4 Incidental personal use of electronic mail, Internet access, fax machines, printers, and copiers is restricted to Regeneronapproved users only and does not include family members or others not affiliated with Regeneron.

1.5.5 Regeneron Information Resources shall not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of any activity that is prohibited by any local, state or federal law.

1.5.6 Regeneron email accounts should not be used to register for personal (non-business-related) services.

1.6 Data Management

The information owned and managed by Regeneron is a valuable asset and needs to be safeguarded just as a physical asset would be. This section provides guidance for the protection of Regeneron's data. Proper data handling helps protect Regeneron from inadvertent loss and loss due to cyber-crime.

1.6.1 All data received, stored, processed, or transmitted on Regeneron's systems are the property of Regeneron.

1.6.2 Users shall not send, upload, remove on portable media, or otherwise transfer to a non-Regeneron system any information that is classified as confidential or higher (or that they should reasonably regard as being classified confidential or higher), except when explicitly authorized to do so in the performance of their regular duties.

1.6.3 Users shall not store Regeneron business information on personal computing devices (e.g. PCs, smart phones, tablets, USB Drives).

1.6.4 The use of portable/removable media is limited to Regeneronsupplied hardware (e.g., USB drives) or approved single/multi-write media (optical or magnetic), provided the media and/or data are appropriately protected.

1.6.5 Users shall not receive, transmit, store, or otherwise access any Regeneron business information via personal email or cloud storage services (e.g. Gmail, Hotmail, iCloud, DropBox, Evernote, etc.). Regeneron may monitor access to any of these types of services, and may temporarily or permanently block them, restricting access at any time.

1.6.6 Users shall not use public instant messaging solutions to transmit Regeneron business information (e.g., WhatsApp, Yahoo Messenger, ICQ, AIM, etc.).

1.6.7 Hard copy information classified as confidential or highly confidential shall not be left unattended in an uncontrolled (nonoffice) environment, or when visitors are present. When possible, information in paper form shall be stored in locked drawers/cabinets.

1.6.8 Hard copies containing data classified as confidential or higher shall be disposed of using controlled disposal mechanisms (e.g. shredders, protected bins).

1.6.9 Paper output shall be promptly retrieved from shared printers and faxes.

1.6.10 Users shall not make unauthorized copies of copyrighted or Regeneron-owned software.

1.6.11 Confidential and Highly Confidential information shall not be shared with any third party unless there is a valid business requirement and the third party's ability to comply with these controls has been verified.

1.7 Identity and Access Management

Keeping your Regeneron identity secure helps protect you from cyber-criminals or inadvertent loss of data. These policy statements serve as guidelines to help safeguard your Regeneron identity, along with any system resources that can be accessed using your credentials.

1.7.1 User accounts shall be unique and associated with a single person for that person's sole use.

1.7.2 Users shall keep passwords secure and not allow others to access their accounts.

1.7.3 Users shall ensure all passwords comply with Regeneron's Password Policy for the type of account used.

1.7.4 Users shall not share their account(s), passwords, personal identification numbers (PINs), security devices (e.g., RSA tokens), or similar information or devices used for identification and authorization purposes.

1.7.5 In the event an end user must disclose a password to technical support staff for support purposes, the user shall change the password immediately following the completion of the support work.

1.7.6 If there is reason to believe user credentials have been compromised or exposed to others, the user shall change the affected password and inform the IT Call Center.

1.7.7 Users should avoid writing down passwords. If this is unavoidable, written passwords should be kept in a secure, locked container (e.g. desk drawer or file cabinet).

1.7.8 Credentials (i.e., username and password) shall not be sent via email. If credentials must be sent to a user for support purposes, an alternate method (e.g., telephone, voicemail, SMS) shall be used.

1.7.9 Standard accounts shall not be granted elevated rights (i.e., local, server, or domain admin). When elevated rights are required, alternate accounts shall be created in order to properly differentiate between end-user functions – such as email and web browsing – and administrative functions (e.g. admin accounts are not to be used for web browsing or accessing e-mail). Accounts shall comply with the Access Management Policy.

1.8 Computing Systems (Server, Workstation, Cloud & Mobile)

As Regeneron data becomes distributed and processed in more locations – such as mobile devices or remote managed services (“The Cloud”), it becomes more important to extend protection to these distributed systems in order to maintain the confidentiality, integrity, and availability of that data.

1.8.1 Users who are supplied with Regeneron-owned equipment (e.g., iPhones, iPads, and laptops) are responsible for the safety and care of the equipment, along with the security of software and data stored on it, and other Regeneron systems that they can access remotely using it.

1.8.2 Users shall not connect non-Regeneron devices to company networks or systems.

1.8.3 Users shall not install or use non-standard software (including freeware, shareware, and browser plug-ins) on Regeneron-owned devices. Exceptions:

*1.8.3.1 Applications (“Apps”) from the Apple App Store are permitted, provided they do not conflict with company policy. Apps that involve the transmission or external storage of Regeneron business information shall be reviewed and approved by Information Security prior to use.*

*1.8.3.2 Users with elevated rights may install software consistent with the approved justification on file for the elevated rights.*

1.9 External Partners and Vendors

Regeneron often utilizes contingent workers through external partners and vendors (“third parties”). While we can outsource work and utilize third-party service providers, extending trust represents additional risk. The following policy statements are guidance for interaction with third parties, and apply to all such relationships, including on-premises and cloud services.

1.9.1 Users shall not engage third-party vendors or services or software to develop, store, or transmit Regeneron business information until they have been reviewed and approved by Information Security.

1.9.2 Third parties shall complete an *InfoSec Technical and Security Questionnaire* prior to engaging into a contract with Regeneron Pharmaceuticals Inc.

1.9.3 Users must have InfoSec approval for each third party solution: approval to provide one service does not imply approval to provide any other services.

1.9.4 Third parties shall be re-assessed when there is a change in the scope of the data or systems involved.

1.9.5 Third parties shall be re-assessed periodically, as specified in the *Third Party Risk Assessment Policy*.

1.10 Reporting

The vigilance of end users is a critical layer of defense against threats that put Regeneron at risk. These policy statements about reporting serve as guidelines to articulate responsibilities and expectations.

1.10.1 Users shall report any confirmed or suspected threats, vulnerabilities, or incidents (e.g. infections, lost equipment, etc.) to their manager and Information Security staff immediately, as these conditions could result in unintentional disclosure of information or exposure to security threats.

1.10.2 Users shall report violations of this Acceptable Use Policy to Information Security Management, who will engage HR and/or Legal as appropriate.

**Noncompliance & Exceptions:**

2.1 Noncompliance

Responses to policy Noncompliance ("violations") may vary. Any noncompliance reported to – or discovered by – Information Security shall be addressed on a case-by-case basis, depending on the severity of the violation and any actual or potential impact.

2.1.1 Disciplinary practice may involve action up to and including termination for serious violations and repeated offenses. Any action taken will be determined by business unit management, HR, and, when necessary, Legal.

2.1.2 Non-Regeneron individuals who violate the Regeneron Information Security Policies may have their access removed or suspended, their company notified, and, if appropriate, legal action taken.

2.1.3 Where noncompliance is found, remediation shall be made to correct the non-compliant state.

2.2 Exceptions

2.2.1 Exceptions may be made to this policy for business purposes, or when compliance is impossible or impractical.

2.2.2 Exceptions shall be approved by Information Security and, where appropriate executive leadership. The approved exception shall be documented.

## FURTHER INFORMATION

The following documents are Regeneron documents related to this policy:

- Password Policy
- Access Management Policy
- Information Security Exception Policy
- Third-Party Risk Assessment Policy

REGENERON
SCIENCE TO MEDICINE®

**POLICY NAME:**

# 240 Monitoring in the Workplace

**Effective Date: 01/01/03**
**Revised Date: 02/20/2020**
**Contact: SECURITY@REGENERON.COM**

## PURPOSE

Regeneron is committed to providing a safe and secure environment.

## SCOPE

This policy applies to all employees of Regeneron. It is also applicable to all clients, service providers, contractors and suppliers of the Company

## POLICY

To ensure our facilities are safe and secure, Regeneron may conduct workplace monitoring. This includes video surveillance, except in areas prohibited by applicable law. Among other reasons, video monitoring is used to:

- identify safety concerns
- monitor safety compliance
- maintain quality control
- deter or detect theft and misconduct
- prevent sabotage
- identify intruders and unauthorized visitors
- discourage or prevent acts of harassment and workplace violence

Regeneron is sensitive to the legitimate privacy concerns of employees, and every effort is made to guarantee that workplace monitoring is done in a discrete, non-intrusive, ethical, and respectful manner.

The Company complies with all applicable privacy laws and regulations.

## FURTHER INFORMATION

For additional information see Information Security: Acceptable Use of Business Information and Information Systems Policy and the other IT Policies.

REGENERON
SCIENCE TO MEDICINE®

**POLICY NAME:**

# 500 Use of and Monitoring of the Telephone, Mail, E-Mail, Camera, Computer and Office Equipment, and Internet Systems

**Effective Date: 01/01/03**
**Revised Date: 01/29/18**
**Contact: ITCOMMUNICATIONS@REGENERON.COM**

## PURPOSE

The purpose of this policy is to state Regeneron's practice regarding monitoring of the telephone, mail, e-mail, camera, computer and office equipment, Internet Systems and any other uses of company resources.

## SCOPE

This policy applies to all employees of Regeneron.

## POLICY

Information assets, including, but not limited to, items such as computers, tablets, telephones, FAX machines, and smart phones, are the property of Regeneron. As such, the data stored on or transmitted through these systems (files, folders, web history, e-mail, text or instant messages, etc.) may be monitored or accessed by the Company. Users of these devices should have no expectation of privacy. The telephone, mail, e-mail, internet systems, computer, and office equipment are provided to conduct Regeneron business in a responsible manner that is consistent and compliant with company policies. Regeneron may, but is not obligated to, conduct workplace monitoring to ensure employee safety, information security, customer satisfaction, billing & cost management, and other purposes.

Casual personal use is permitted, provided it is also consistent and compliant with company policy and applicable laws. Regeneron requires all employees comply with the Equal Employment Opportunity Policy, the Anti-Harassment Policy, Information Security Policies (available on the Intranet in the IS section) and all other relevant Regeneron policies while using these systems.

Employees may be required to reimburse Regeneron for any charges resulting from their personal use of these services. If personal use is determined to be abusive or inappropriate, employees may be subject to disciplinary action, up to and including termination of employment.

Use of cameras, camera phones, and other audio/video recording equipment for business purposes must follow pre-approval by the Legal Department. Casual personal use of these devices/features must also comply with all appropriate company policies, as well as federal, state and local law.

Mail and shipping services to and from Regeneron's business locations are for company business use only.

REGENERON
SCIENCE TO MEDICINE®

## FURTHER INFORMATION

For more information related to mail, shipping or telephone services please call the VP of Facilities at extension #7407, at IOPS contact the BMRAM coordinator and Admin.