Egan-Jones Ratings Company
("EJR")

Form NRSRO

Exhibit #3: Policies or Procedures adopted and implemented to prevent the misuse of material, nonpublic information

- **Code of Conduct**
- **EJR Conduct and Compliance Manual (Sections of the Manual listed below were adopted and implemented to prevent the misuse of material, nonpublic information)**
  - **Handling of Confidential Information and Non-Public Information**
  - **Separation between Ratings and Marketing**
  - **Separation between Compliance and Marketing**
  - **Procedure for Internal Role Changes**
  - **Separation between Ratings and Proxy**
  - **Personal Securities Transactions and Holdings**
  - **Outside Business Activity Reviews**
  - **Standard for E-Mail Addresses**
  - **Standards Governing Approved as well as Off-Channel Communications Platform**
- **Types of Credit Ratings Policy**
- **Information Security Policy**

Code of Conduct
(Code of Conduct Effective 06/30/2023)

Dear Colleagues,

As global events such as the pandemic have changed the way people around the world work and interact with one-another, Egan-Jones remains committed to doing business and serving clients with integrity and in accordance with the highest ethical standards. Whether you work remotely, in an Egan-Jones office setting, or in a hybrid work environment, each of us is responsible for understanding and following the Code of Conduct and all other applicable policies and procedures. This updated Code of Conduct is a critical component of the Company's internal control structure. Please be sure to familiarize yourself with, and attest to, this Code of Conduct and other relevant policies and procedures contained on EJ System, and complete all required training sessions throughout the year.

If you have any questions regarding the Code of Conduct or related matters, please contact your manager or the Compliance Department. If you become aware of violations of this Code of Conduct, law, or regulation, you may report them to your manager and to the Compliance Department. Thank you for your ongoing commitment to ethics and integrity.

Sincerely,

Don Howard
Independent Chairman of the Board

Sean Egan
CEO

Michael Brawer
Designated Compliance Officer

Table of Content

EGAN-JONES RATINGS COMPANY CODE OF CONDUCT ..... **Error! Bookmark not defined.**

PRINCIPLES OF THE CODE 4

Statement on Core values and Mission 4

Fostering a Culture of Compliance 4

Know and Understand the Laws and Regulations 5

Professionals Serving Professionals 5

Trust, but Verify 5

ACT IN THE BEST INTERESTS OF THE FIRM, CLIENTS & THE PUBLIC 5

Fair Dealing & Integrity 5

Personal Email Usage Policy and Off-Channel Communications 5

Conflict of Interest 6

Examples of Conflicts of Interest that can be Managed and Disclosed *7*

Examples of Prohibited Conflicts of Interest *8*

Identified Conflicts of Interest *10*

Gifts & Entertainment 11

Corporate Opportunities 11

Firm Systems and Assets 12

Personal Securities Transactions and Holdings 12

Insider Trading Policies and Procedures 13

ENFORCEMENT AND ADMINISTRATION OF THE CODE 14

What to Do if You Learn Inside Information 14

How to Preserve the Confidentiality of Material Non-Public Information 14

Provide Fair and Truthful Disclosures to Our Clients & the Public 15

Reporting Violations 15

Policy Against Retaliation 15

Measures to be Undertaken in the Event of a Material Breach 15

Consequences of Violating the Code 16

Attestation, Waivers, Amendments and Contact Information 16

EGAN-JONES RATINGS COMPANY
CODE OF CONDUCT

PRINCIPLES OF THE CODE

Statement on Core values and Mission

The mission of Egan-Jones Ratings Company ("EJR" or the "Firm") is to provide market participants with timely and accurate credit ratings and other services. EJR serves clients in the private debt markets, as well as certain other markets, by providing analytical insights in a clear and concise format. As a market leader in the provision of private credit ratings, all ratings are based on sound analytical methodologies. The firm's other services are similarly provided in accordance with robust procedures and methodologies.

The firm's values are centered on analytical integrity and independence. Analytical methodologies are developed by industry experts with relevant skills and experience in an environment that is free from inappropriate commercial influence.

As a regulated credit rating agency, compliance is afforded the highest priority at Egan-Jones. The Firm has established a system of internal controls to ensure an exceptionally high level of compliance with applicable laws and regulations.

EJR is committed to fostering a work environment that allows the views of its Associated Persons to be expressed in a committee or other consensus-oriented setting. For example, committee voting will take place after voting members have each had an opportunity to express their views.

Fostering a Culture of Compliance

The Firm has a Code of Conduct (the "Code"), which serves as its code of ethics. The purpose of this Code is to set forth basic principles to guide you in your day-to-day activities as an Associated Person, and to outline the expectations the Firm has of all its Associated Persons. The Firm requires its Associated Persons to read and adopt the Code to enhance their understanding of the Firm's practices, including procedures regarding personal securities and money market instruments transactions, insider trading and personal email usage provisions. This Code is intended to provide basic principles and behavior guidelines and foster a "culture of compliance" at EJR.

The Code does not cover every regulatory, legal, or ethical issue that you may confront at the Firm. Indeed, no code of conduct can attempt to anticipate the myriad of issues that arise in a fast-moving, financial-related enterprise like EJR. However, by following this Code and the Firm's policies and procedures, by adhering to the letter and the spirit of all applicable laws and regulations, and above all, by applying sound judgment to your activities, the Associated Persons will be able to adhere not only to the regulatory requirements applicable to EJR, but also to the Firm's commitment to compliance and ethical behavior in all of its activities.

In addition to this Code, you are required to read and acknowledge acceptance of, and compliance with, the EJR Conflicts and Compliance Manual (the "Manual"). The Manual contains additional information on the regulations governing NRSROs, issues that are presented in the operation of a credit ratings business— most notably, conflicts of interest, and other subjects that may or may not be addressed in this Code.

Know and Understand the Laws and Regulations

EJR is registered as a nationally recognized statistical rating organization ("NRSRO") with the U.S. Securities & Exchange Commission ("SEC" or the "Commission") in the following classes of credit ratings: (1) financial institutions, brokers or dealers; (2) insurance companies; and (3) corporate issuers, and is therefore subject to regulation and oversight in the United States by the Commission. EJR is also subject various laws of the Commonwealth of Pennsylvania where its main office is located as well as state and local laws of each of EJR's offices. It is your responsibility to know and understand the laws and regulations applicable to your job responsibilities, and to comply with both the letter and the spirit of these regulations, as well as the Firm's policies and procedures. EJR requires that you avoid not only any actual misconduct but also even the appearance of impropriety. We require Associated Persons to rely on common sense, good judgment, individual integrity and a discerning mind to guide you in your day-to-day activities. Assume that any action you take ultimately could be publicized; therefore, when taking an action consider how you and the Firm would be perceived. When in doubt, seek guidance from the Firm's knowledgeable regulatory and compliance personnel. Such personnel will assist you in obtaining any guidance you might need.

Professionals Serving Professionals

EJR provides credit rating products and services for institutional clients. The majority of its clients have long-term high-level experience within the securities business, and have internal capability for independent analysis and investment decision making. Our product is a tool for such professional institutional clients.

Trust, but Verify

Trust your instincts. If something does not appear to be lawful or ethical, or you have a question about it, ask the Firm's Designated Compliance Officer ("DCO"), raise a flag, and ask for help from the Firm's resources. Seek guidance rather than making assumptions that you are aware of regulatory nuances. The Firm strongly encourages you to discuss freely any concerns with knowledgeable persons, and requires you to report to the Compliance Department violations of law and regulation as well as internal policies and procedures. If you are unclear about the applicability of regulations to your job responsibilities, or if you are unsure about the propriety of a particular course of action, you should seek the advice of your supervisor and / or the Firm's DCO. You should never assume that an activity is compliant merely because others in the industry engage in it or you do not see any pitfalls in the course of action. EJR encourages you to reach out to any of the foregoing with your questions prior to pursuing a course of action if you are not 100% positive you know the regulatory ramifications of that action.

ACT IN THE BEST INTERESTS OF THE FIRM, CLIENTS & THE PUBLIC

Fair Dealing & Integrity

The Firm's basic core concept is that we provide a valuable service to our institutional clients. We rely on the trust of our clientele, for their belief and respect for our products and services, and the trust they invest in our abilities and integrity. The Firm seeks to outperform its competition fairly and honestly through timely superior analysis and experience. Every Associated Person must therefore always keep the best interests of the Firm's clients paramount and endeavor to fairly and properly deal with its clients, competitors, public, and vendors. No one should take unfair advantage of anyone through manipulation, abuse of privileged information, misrepresentation of facts, intimidation, or any other unfair practice. No Associated Persons should ever position themselves for, or take, personal gain through their association with the Firm.

Personal Email Usage Policy and Off-Channel Communications

As discussed more broadly in EJR's Conflicts and Compliance Manual and Information Security Policy, EJR maintains standards governing approved communications devices and channels, as well as unapproved communications devices and channels which include use of any personal or non EJR controlled communication device or channels ("Off-Channel Communications"). Associated persons are expected to read and be familiar with policies and procedures prohibiting the use of Off-Channel Communications, such as SMS/text messages, encrypted mobile phone messaging, and personal e-mail accounts for business purposes.

EJR's Associated Persons are strictly prohibited from using their personal email accounts to transmit and/or receive confidential information and/or confidential workplace documents or to conduct workplace business, provided certain limited exceptions may be granted by the Compliance Department for Associated Persons working from home. The Code of Conduct attestation includes a clause requiring all EJR Associated Persons to attest to use only their EJR email address to transmit and/or receive Confidential Information and/or confidential work papers or to conduct workplace business. Attestations are collected and reviewed by the Compliance Department. As part of the Firm's annual compliance training, all Associated Persons will be reminded of EJR's policies and procedures with regards to safeguarding confidential information and material nonpublic information.

On a periodic basis, the Compliance Department will conduct an email search on randomly-selected Associated Persons to ensure emails sent to or received from personal email accounts did not contain Confidential Information and/or confidential workplace documents (see "Email Review Policies and Procedures" in the Conflicts and Compliance Manual). Email search results will be retained within a compliance surveillance folder. Any Associated Persons who use a personal email account are required to attest to their awareness of this Personal Email Usage Policy. Associated Persons who commit an infraction of this Policy may be subject to disciplinary action, including termination at the recommendation of the DCO.

Associated Persons are also prohibited from using the Firm's email to transmit material that may be deemed to be offensive to a prudent person, or emails that reflect badly on the corporate culture of the Firm. Those include (but are limited to) any email that could be deemed pornographic, sexist, hateful, racist, discriminatory, terroristic, harassing, disparaging to the Firm or any of its Associated Persons, or any email that could be considered workplace brutality. Any emails with the aforementioned content will not be tolerated in the Firm's email environment, and may lead to immediate disciplinary action, including termination. Note that these email policies also apply to personal email accounts accessed via the Firm's systems.

Conflicts of Interest-- Background

Broadly speaking, there are two categories of conflicts of interest that associated persons need to be aware of:

1) Conflicts of interest that can be managed and disclosed; and
2) Prohibited conflicts of interest

Below is an overview of both types of conflicts. Associated Persons should read and be familiar with EJR's Conflicts and Compliance Manual, which provides significant additional information pertaining to conflicts of interest and how EJR manages and/or avoids conflicts through its system of internal controls.

In addition to being paid by issuers and subscribers, the NRSRO is also paid to determine ratings by investors and asset managers. Frequently these engagements contemplate the issuance of the credit rating on a private basis. In these cases, the NRSRO provides the credit rating directly to its client but does not publish (or make available to all its subscribers) the credit rating or a report detailing its credit analysis (although such a report may be provided to the client with the rating). This business model is subject to conflicts of interest, which are oftentimes related to the objectives of the client for obtaining the rating.

As discussed above, in addition to conflicts of interest that must be managed and disclosed, the Securities and Exchange Commission prohibits certain conflicts of interest relating to the issuance of credit ratings by an NRSRO. The Commission believes this regulation is necessary and appropriate in the public interest and for the protection of investors because it addresses a practice that could impair the objectivity, and, correspondingly, the quality, of a credit rating. Commission believes the prohibition creates a strong incentive for NRSROs to improve their disclosures, which, in turn, will benefit the users of credit

ratings and, by extension, the credit markets.

Section 15E and the related Commission rules address conflicts of interest. For example, Rule 17g-5 identifies certain conflicts of interest that are prohibited under all circumstances (Rule 17g-5(c)) and other conflicts of interest that are prohibited unless an NRSRO has publicly disclosed the existence of the conflict and has implemented policies and procedures reasonably designed to address and manage such conflict (Rule 17g-5(b)(1)-(10)).

Consistent with applicable regulatory requirements, EJR establishes and maintains a system of internal controls to ensure that applicable staff maintain EJR's analytical independence and avoid prohibited conflicts. EJR Associated Persons are prohibited from engaging in any activity that might constitute or result in, or create the appearance of, any impropriety or conflict of interest.

The primary responsibility of EJR Associated Persons is to perform their jobs in an efficient, compliant and productive manner. EJR Associated Person are expected to meet EJR's standards of work performance and personal conduct, including following company rules and adhering to established internal controls and working practices.

Conflict disclosure- When an Associated Person becomes aware of an actual or potential conflict of interest, they are responsible for taking appropriate action in accordance with legal and regulatory requirements and EJR's policies and procedures. For example, EJR Associated Persons are required to disclose to their supervisors and the EJR Compliance Department their involvement with any transaction or business relationship that might reasonably give rise to an actual conflict of interest or the appearance of a conflict of interest.

Examples of Conflicts of Interest that can be Managed and Disclosed

Many of EJR's clients have an economic interest in achieving a particular rating level. This creates a conflict of interest that needs to be managed and disclosed. Such conflicts are disclosed on Form NRSRO. Examples of EJR clients who may have an economic interest in achieving a particular rating level can include:

- Issuers
- Underwriters
- Obligors
- Entities that may own investments or have entered into transactions that could be impacted by a credit rating issued by EJR
- Clients who may use credit ratings to comply with, and obtain benefits or relief under, statutes and regulations using the term "nationally recognized statistical rating organization."
- Subscription clients who may own investments or have entered into transactions that could be favorably or adversely impacted by a credit rating issued by EJR.

Many of the above conflicts fall, broadly speaking, under the "issuer-pays" business model. To help manage these sorts of conflicts and ensure the integrity and independence of EJR's credit ratings, EJR segregates various functions. The most fundamental aspect of this segregation entails the segregation of Analytical and Sales/Marketing roles. Analytical staff are not permitted to become involved in sales or marketing activities and Sales/Marketing staff are not permitted to influence Analytical staff. As an example, it is not appropriate for Sales/Marketing staff to share with Analytical staff any information pertaining to fees or contract terms or to indicate to Analytical staff that a particular client is important to the firm. Beyond role segregation, EJR also physically segregates Analytical and Sales/Marketing staff during times when both roles may be located in a physical office setting. Finally, data and information segregation is enforced so that each role views information pertinent to their legitimate business purposes.

Where clients purchase multiple products from a rating agency (for example, credit ratings and proxy services) this has the potential to give rise to conflicts of interest. This general type of conflict is disclosed on Form NRSRO and, as specific instances are identified in course of regular monitoring performed by Ratings Sales staff, those instances are disclosed on the 17g-7

Disclosure Form pertaining to the relevant rating action.

Associated persons are allowed to own securities of issuers or obligors subject to a credit rating determined by EJR as long as they do not participate in or influence such credit ratings. This is disclosed on Form NRSRO. EJR employs an array of controls, including systems-based controls that help prevent analysts from voting in a rating committee where their personal securities holdings may pose a conflict of interest. In addition, EJR's Compliance team collects and reviews brokerage statements to help enforce the more detailed guidance set out below.

EJR allows persons within EJR to have a business relationship that is more than an arm's length ordinary course of business relationship with issuers or obligors subject to a credit rating determined by EJR as long as they do not participate in or otherwise influence the credit rating for such issuers or obligors. This is disclosed on Form NRSRO. EJR's Compliance Department administers Outside Business Activity (OBA) disclosure forms and, where necessary, conducts follow up interviews with associated persons in order to manage any potential conflicts of interest that may arise in connection with outside business relationships.

Examples of Prohibited Conflicts of Interest

As an NRSRO, the Firm is prohibited under Rule 17g-5(c) of the Securities Exchange Act of 1934, as amended ("Exchange Act") from having the following conflicts of interest relating to the issuance or maintenance of a credit rating as a credit rating agency, and we therefore do not engage in the PROHIBITED CONFLICTS listed below:

(1) Issue or maintain a credit rating solicited by a person that, in the most recently ended fiscal year, provided the Firm with net revenue (as reported under §240.17g-3) equaling or exceeding 10% of the total net revenue of the Firm for the fiscal year;[1]

EJR's Accounting team performs monitoring and reporting of client net revenues. Compliance and other firm leadership, as well as EJR's Board of Directors, receive reports and conduct oversight to help ensure that this prohibited conflict is not violated.

(2) Issue or maintain a credit rating with respect to a person (excluding a sovereign nation or an agency of a sovereign nation) where the Firm, a credit analyst that participated in determining the credit rating, or a person responsible for approving the credit rating, directly owns securities of, or has any other direct ownership interest in, the person that is subject to the credit rating.

Please refer to "Personal Securities Transactions and Holdings" herein for detailed information.

(3) Issue or maintain a credit rating with respect to a person associated with the Firm; or Issue or maintain a credit rating where a credit analyst who participated in determining the credit rating, or a person responsible for approving the credit rating, is an officer or director of the person that is subject to the credit rating;

The Compliance Department administers and reviews outside business activity disclosure forms. Where potential risks are identified on outside business activity disclosure forms, Compliance will conduct additional inquiries/interviews with staff in order to effectively identify and restrict certain activities, as necessary and appropriate.

(4) Issue or maintain a credit rating with respect to an obligor or security where the Firm or a person associated with the Firm made recommendations to the obligor or the issuer, underwriter, or sponsor of the security about the corporate or legal structure, assets, liabilities, or activities of the obligor or issuer of the security;

The purpose of this rule is to address the potential lack of impartiality that could arise when an NRSRO determines a credit rating based on a corporate structure that was developed after consultations with the NRSRO or its affiliate on how to achieve a desired credit rating. In simple terms, the rule prohibits an NRSRO from rating its own work or the work of an affiliate.

The following specific example pertaining to structuring may surface when dealing with clients:

When a client requests an NRSRO rating that the Firm cannot rate due to the Firm's NRSRO registration status (e.g., a request for a rating on a municipal security, government security, foreign government security or ABS security), you must inform the client that the Firm is unable to provide an NRSRO rating for such security because the Firm is not registered as an NRSRO in respect of such class(es) of credit ratings. You may not make any suggestions or recommendations to the client about ways in which the security could provide an NRSRO rating.

(5) Issue or maintain a credit rating where the fee paid for the rating was negotiated, discussed, or arranged by a person within the Firm who has responsibility for participating in determining credit ratings or for developing or approving procedures or methodologies used for determining credit ratings, including qualitative and quantitative models; or Issue or maintain a credit rating where a person within the Firm who participates in determining or monitoring the credit rating, or developing or approving procedures or methodologies used for determining the credit rating, including qualitative and quantitative models, also:

i. Participate in sales or marketing of a product or service of the Firm or a product or service of an affiliate of the Firm; or

ii. Is influenced by sales or marketing considerations.

The purpose of this rule is to remove the persons directly involved in making the judgments that credit ratings are based on from fee negotiations and, thereby, insulate them from considerations that could make them more or less favorably disposed toward a client or class of clients. It is essential to insulate rating analysts from business pressures by separating rating agencies' business-development function from their analytical function.

In addition to controls pertaining to the segregation of roles and information (discussed above and in EJR's Conflicts and Compliance Manual), EJR maintains 'tainted procedures', effectively providing for a cooling-off period where Analytical staff inadvertently come into contact with commercial information (e.g., fee information, contract terms).

(6) Issue or maintain a credit rating where a credit analyst who participated in determining or monitoring the credit rating, or a person responsible for approving the credit rating received gifts, including entertainment, from the obligor being rated, or from the issuer, underwriter, or sponsor of the securities being rated, other than items provided in the context of normal business activities such as meetings that have an aggregate value of no more than $25 (See Section "Gifts & Entertainment" below).

The purpose of this rule is to eliminate the potential for undue influence that gifts and entertainment can have on those responsible for determining credit ratings.

Please see guidance pertaining to gifts and entertainment below and more detailed guidance in the Conflicts and Compliance Manual.

For the purposes of the above Prohibited Conflicts, the term person within an NRSRO means the Firm itself, its credit rating affiliates identified on Form NRSRO, and any partner, officer, director, branch manager, and employee

(including all Associated Persons) of the Firm or its credit rating affiliates (or any person occupying a similar status or performing similar functions). Any questions with respect to the meaning or scope of such conflicts should be referred to the Compliance Department.

As discussed above, EJR maintains a comprehensive system of internal controls. This system of internal controls is documented and maintained by the Compliance Department. Some examples of internal controls intended to help the organization avoid certain prohibited conflicts of interest include:

Prohibited conflict pertaining to clients who could provide the NRSRO with net revenue equaling or exceeding 10% to the total net revenue of the NRSRO for the fiscal year.

Internal control: Accounting periodically monitors and circulates a report showing year-to-date net revenue by client/revenue type. The 10% analysis report is used for the purpose of monitoring adherence to Rule 17g-5(c)(1). Compliance and senior management review the report and propose appropriate action, as necessary.

Example of prohibited conflict dealing with personal securities holdings: An analyst that participates in the rating process for XYZ Inc. may not hold securities of XYZ Inc.

Internal Control: New Associated Persons submit their securities holdings along with brokerage statements as part of EJR's onboarding procedures. Associated Persons submit applicable brokerage account statements to the Compliance Department on a quarterly basis. Analyst(s) are required to attest that they do not have any prohibited conflicts prior to determining credit ratings.

Prohibited conflict: Credit rating analysts are not permitted to negotiate ratings fees.

Internal control: EJR ratings analyst(s) are strictly prohibited from discussing fee information, types/structures of fees, or any other fee-related information, even if the specific amount is not discussed.

Public Disclosure of Identified Conflicts of Interest and Related Conflict Procedures

Under Rule 17g-5(b)(1)-(10) of the Securities Exchange Act of 1934, as amended ("Exchange Act") EJR has adopted internal procedures and mechanisms to identify and eliminate, or to manage and disclose, as appropriate, actual or potential conflicts of interest that may influence the opinions and analyses EJR makes or the judgment and analyses of EJR Associated Person involved in credit rating activities or who approve credit ratings and rating outlooks.

(1) EJR is paid by issuers or underwriters to determine credit ratings with respect to securities or money market instruments they issue or underwrite.

(2) EJR is paid by obligors to determine credit ratings with respect to the obligors.

(3) EJR is paid by entities to determine credit ratings with respect to obligations of third parties where such entities may own investments or have entered into transactions that could be impacted by a credit rating issued by EJR.

(4) EJR is paid for services in addition to determining credit ratings by issuers, underwriters, or obligors that have paid EJR to determine a credit rating.

(5) EJR is paid by persons for subscriptions to receive or access the credit ratings of EJR and/or for other services offered by EJR where such persons may use the credit ratings of EJR to comply with, and obtain benefits or relief under, statutes and regulations using the term "nationally recognized statistical rating organization."

(6) EJR is paid by persons for subscriptions to receive or access the credit ratings of EJR and/or for other services offered by EJR where such persons also may own investments or have entered into transactions that could be favorably or adversely impacted by a credit rating issued by EJR.

(7) EJR allows persons within EJR to directly own securities or money market instruments of, or having other direct ownership interests in, issuers or obligors subject to a credit rating determined by EJR as long as they do not participate in or otherwise influence the credit rating for such issuers or obligors.

(8) EJR allows persons within EJR to have a business relationship that is more than an arm's length ordinary course of business relationship with issuers or obligors subject to a credit rating determined by EJR as long as they do not participate in or otherwise influence the credit rating for such issuers or obligors.

Policies, procedures and internal controls associated with the above identified conflicts of interest are also discussed in EJR's Conflicts and Compliance Manual.

EJR has also disclosed certain of its conflict avoidance and management measures on its free public website at https://www.egan-jones.com. EJR's disclosures of known actual and potential conflicts of interest shall be timely, clear, concise, specific, and prominent. Please refer to Exhibit 6, "Identification of Conflicts of Interest Relating to the Issuance of Credit Ratings," and Exhibit 7, "Policies and Procedures to Address and Manage Conflicts of Interest," to Form NRSRO, which are available on the Firm's website, www.egan-jones.com/nrsro, for a description of policies and procedures which must be followed by Associated Persons in relation to conflicts of interest.

Gifts & Entertainment

Gifts and entertainment may create an inappropriate expectation or feeling of obligation. You are required to follow gifts standards detailed in the NRSRO rules and note that gifts that fall outside the standard are prohibited. You and members of your family may not accept gifts or gifts offered in the form of cash or cash equivalents, or special favors (other than an occasional non-cash gift of nominal value – i.e., coffee mugs with logos, etc.) from any person or organization with which the Firm has a current or potential business relationship or from any Company that the Firm does or may rate. Further, business gifts to, and entertainment of, non-government employees in connection with business discussions or the development of business relationships are only appropriate if they are in the ordinary course of business and their value is modest. If you have any questions about the appropriateness of a business gift or expense, you should contact your supervisor or the DCO. Associated Persons are required to receive preapproval from the Compliance Department before giving gifts and any gifts which are received need to be reported to the Compliance Department to ensure the gift is appropriate per NRSRO rules. Detailed guidance pertaining to gifts and entertainment is provided in EJR's Conflicts and Compliance Manual.

Giving gifts to, or entertaining, government employees (including employees of international organizations and or regulatory bodies) may be prohibited. The United States Foreign Corrupt Practices Act, for example, prohibits giving anything of value, directly or indirectly, to any "foreign official" for the purpose of obtaining or retaining business. Check with your supervisor or the DCO if you have any questions about the acceptability of conduct in any foreign country, including contacting foreign officials with respect to the Firm's sovereign ratings or the sales of Firm products to foreign governments or agencies.

Corporate Opportunities

As an Associated Person, you owe a duty to the Firm to advance its interests. No Associated Person may use their position or corporate property or information for personal gain. Additionally, no Associated Person may take for themselves the Firm's opportunities for sales or purchases of products, services or interests. Business opportunities that arise as a result of your position in the Firm or through the use of corporate property or information belong to the Firm.

Firm Systems and Assets

The Firm's policies regulate use of the Firm's systems, including telephones, computer networks, electronic mail, and remote access capabilities. Generally, you should use the Firm's systems and properties only for legitimate Firm business. Under no conditions may you use the Firm's systems to view, store, or send unlawful, offensive or other inappropriate materials. In addition, protecting the Firm's assets against loss, theft, waste, or other misuse is the responsibility of every Associated Person. Any suspected misuse should be reported to your supervisor or the DCO.

Personal Securities Transactions and Holdings

The Firm's personal securities policy is designed to address potential conflicts of interest in cases where Associated Persons have ownership positions in issuers or related entities the Firm does or may do business with. This policy applies to accounts of the Associated Person and the Associated Person's direct family members. As used herein, direct family members includes an Associated Person's spouse and minor and dependent children and references should be interpreted accordingly. If there are questions about whether someone constitutes a direct family member, the Associated Person should speak with the Compliance Department.

An Associated Person must disclose brokerage or other investment accounts, including private investments, trusts or investment clubs, in which the Associated Person has direct or indirect influence or control (such as joint ownership, trading authorization, or the authority to exercise investment discretion) or a direct or indirect beneficial ownership interest. Accounts related to money market instruments and commercial paper are also subject to this Personal Securities Transactions and Holdings policy. Notwithstanding the foregoing, an Associated Person is not required to disclose the following types of accounts or accounts that can only hold the following types of investments: open-end mutual funds; foreign exchange; cryptocurrency; pension or retirement accounts in which the Associated Person does not have investment discretion and where the Associated Person is not permitted to invest directly in securities; commodities; futures on commodities, currencies and indices; certificates of deposit; bank accounts; 529 accounts or plans; and 401K or similar retirement accounts that are not able to hold individual securities or closed-end funds. Trusts or similar investment vehicles managed by a third-party, including blind trusts, where the Associated Person has no direct or indirect influence or control over the trust or account ("Third-Party Accounts") are permitted provided Associated Persons and their immediately family members utilize such accounts to trade exclusively in open-ended funds and ETFs, and that such accounts may not and do not buy, hold, or sell individual securities or bonds. All Associated Persons are required to disclose all applicable personal securities accounts and holdings, including US and non-US (China, India etc.) accounts and holdings, and, if possible, ask their account custodian to send "duplicate" or "interested party" statements to the Firm's Compliance Department.

The purchase, sale and holding of individual equity and/or fixed income securities, including options on such securities and exercise of such options, and closed-end funds is prohibited. The purchase, sale and holding of ETF's is permissible without preclearance. As a best practice, new Associated Persons should liquidate pre-existing positions in non-Third-Party Accounts. The Firm recognizes that liquidations may incur transaction fees and have unwanted tax consequences in taxable accounts. Affected Associated Persons may request a limited waiver from this provision of the Code from the DCO. Waiver requests must be in writing. Should the Associated Person wish to liquidate a position in respect of which a waiver had previously been granted, he/she must request, and receive, pre-clearance approval from the DCO, noting the name of the security, ticker symbol or CUSIP, and size of the position to be liquidated. The DCO will check with the Firm's Ratings Group to make sure the Firm has no active engagements or outstanding work with the issuer or the security involved, and, if there are no other potential conflicts identified, open up a trading window during which the Associated Person can make the trade. DCO trading approvals generally are valid for five business days unless specified.

Compliance Guidance: Accounts with discretionary authority should not have the ability to trade or hold individual securities.

Insider Trading Policies and Procedures

NRSRO firms are required to establish, maintain, enforce, and document policies and procedures to prevent the misuse of material non-public information ("MNPI"). MNPI generally includes (a) information that is not generally known to the public about the Firm, its clients, or other parties with whom the Firm has a relationship and that have an expectation of confidentiality ("Confidential Information"); and (b) non-public information that might be useful to competitors or that could be harmful to the Firm or its customers if disclosed, such as, the names of clients, intellectual property, IT security systems, business plans, personal employee information and unpublished financial information ("Proprietary information" or, collectively, "Inside Information").

Inside Information generated and gathered in our business is a valuable asset of the Firm. Protecting Inside Information is critical to the Firm's reputation for integrity and its relationship with its clients, and ensures the Firm's compliance with the complex regulations governing the financial services industry. Accordingly, you should maintain all such information in strict confidence. You should also respect the property rights, including Inside Information, of other companies.

Unauthorized use or distribution of Inside Information violates the Firm's internal policy and could be illegal. Such use or distribution could result in negative consequences for both the Firm and the individuals involved, including potential legal and disciplinary actions. Your obligation to protect the Inside Information you come into contact with continues even after you leave the Firm, and you must return all documents containing such information in your possession to the Firm upon your departure.

If Associated Persons receive Inside Information, they are prohibited from securities trading ("Insider Trading"), whether for the account of themselves, their family, friends, or any customer, any accounts in which they have a direct or indirect beneficial interest (including accounts for family members) and any other account over which they have control, discretionary authority or power of attorney and any account on their behalf. This absolute trading prohibition is in effect should the Firm cover that issuer or not. Additionally, Associated Persons are prohibited from sending or sharing Inside Information to others. Insider Trading for these purposes is any trading activity where persons trade while in possession of material information that is not known to the investing public and which provides the holder or recipient of the information with a potentially unfair advantage in the marketplace.

The penalties for Insider Trading can be considerable, including loss of profits plus damages, criminal sanctions including incarceration, loss of employment and permanent bar from the securities industry. If you are in possession of Inside Information about a company or the market for a company's securities, you must refrain from acting upon it. You also may not communicate Inside Information to another person who has no official need to know it.

If you are in possession of Inside Information, you are required to safeguard it based on a "legitimate business need to know" standard, and to promptly notify the DCO of any inappropriate internal or external dissemination Please see NRSRO Exhibit 3: Policies or procedures adopted and implemented to prevent the misuse of material, nonpublic information., which is reasonably designed to prevent the misuse of Inside Information considering the Firm's business, structure, size and other relevant factors. The Firm recognizes that in the course of its work it may be exposed to Inside Information so all Associated Persons must be able to identify material non-public information and handle such information properly.

The Firm anticipates that instances of exposure to Insider Information may occur, including inadvertently, in the course of research activities. For instance, company projections often constitute material non-public information. Any kind of trading while in possession of Inside Information may constitute Insider Trading and, at a minimum, may be improper, if not illegal. In addition, trading while in possession of information concerning the pending issuance of a rating by the Firm (front-running) is also prohibited. These activities are STRICTLY PROHIBITED.

In addition, all of the Firm's credit analysis work is highly confidential and proprietary information and shall not be disclosed. The Firm's decision to upgrade, downgrade or, in some cases, review or update a rating on a security or an instrument, may be material non- public information and thus is to be very closely guarded prior to the rating publication. No ratings action decision should ever be disclosed, prior to dissemination, to anyone outside of the Credit Analysts at the Firm.

Compliance Guidance: Double-check the accuracy of auto-filled e-mail addresses prior to clicking Send.

ENFORCEMENT AND ADMINISTRATION OF THE CODE

What to Do if You Learn Inside Information

It is not illegal to learn Inside Information. The Firm or its Associated Persons may learn material non-public information from its clientele or in thecourse of its ratings work. It is, however, illegal for you to act or trade while in the possession of such information, or to pass it on to others other than the DCO of the Firm. You should tell the DCO that you are in receipt of such information for the purpose of sequestering the information and making sure it does not affect any ratings decision.

If you believe you have learned Inside Information, contact the Firm's DCO immediately so that they may address all potential issues and preserve the integrity of the Firm's commitment to information handling. If you become aware of a breach of these policies or of a leak of Inside Information, advise the Firm's DCO immediately. You must refrain from distributing that information to others, make sure it is not openly available on your computer and sequester it within your email to prevent easy accessibility by others.

How to Preserve the Confidentiality of Material Non-Public Information

The following are non-exclusive steps you must take to preserve the confidentiality of non-public information:

- Do not discuss confidential matters (in person or via phone) in elevators, hallways, restaurants, airplanes, taxicabs or any place where you can be overheard.
- Do not leave sensitive memoranda on your desk or in other places where they can be read by others. Do not leave a computer terminal without exiting the file in which you are working.
- Do not read confidential documents in public places or discard them where they can be retrieved by others. Do not carry confidential documents in an exposed manner.
- On drafts of sensitive documents use redacted names if necessary.
- Do not discuss confidential business information with spouses, other relatives or friends.
- Avoid even the appearance of impropriety. Serious repercussions may follow from insider trading or using non-public information to benefit yourself or another. You should consult with Compliance whenever you have questions about this subject.
- Shred confidential documents that are no longer needed per the Firm's document and record retention policies

At no time may the Firm or any member of the Firm discuss or disclose such information or perform any personal securities and money market instruments transactions related to MNPI until the MNPI is in the public domain or otherwise is no longer material.

The Firm has a vital interest in its reputation, the reputation of its Associated Persons, and in the integrity of the securities

markets. Trading while in possession of inside or confidential Firm information would destroy that reputation and integrity. The Firm is committed to preventing this conduct and to punishing any Associated Person who engages in this practice or fails to comply with the above steps designed to preserve confidentiality of Inside Information. These procedures are a vital part of the Firm's compliance efforts and must be adhered to.

Provide Fair and Truthful Disclosures to Our Clients & the Public

The Firm has a responsibility under the law to communicate effectively so that its clients are provided with full and accurate information in all material respects. To the extent that you are involved in the preparation of materials for dissemination to clients, you should be careful to ensure that the information in these materials is truthful, accurate and complete. In particular, the Firm's officers and directors shall endeavor to promote full, fair, accurate, timely and understandable disclosure in the Firm's communications, including documents that the Firm files with or submits to the SEC Staff and other regulatory bodies. If you become aware of a materially inaccurate or misleading statement in any communication to the Firm's clients, the SEC Staff, other regulatory bodies, or the public, you should report it immediately to your supervisor and the Compliance Department.

Reporting Violations

You are the Firm's first line of defense against unethical or improper business practices. If you observe or become aware of any conduct that you believe is unethical or improper - whether by another employee, a consultant, a supplier, a client, or other third party - you must communicate that information to the Firm's ownership, compliance officer (DCO), counsel, or to the 24-hour independently operated helpline. They will take appropriate action. If you are a supervisor, you have an additional responsibility to take appropriate steps to stop any misconduct that you are aware of, and to prevent its occurrence and/or recurrence. Supervisors that do not take appropriate action may be held responsible for failure to supervise properly. If you prefer to report an allegation anonymously, you must provide enough information about the incident or situation to allow the Firm to investigate properly.

Individuals – whether they are located in the U.S. or in other jurisdictions – have the option to report concerns or possible violations through an independent third-party that specializes in the discrete reporting of integrity concerns, and are available 24 hours a day, seven days a week. The telephone number to the independent helpline is 1-484-789-6596. Calls to the helpline may be made anonymously or on a disclosed basis.

Credit rating agencies must disclose and manage certain types of conflicts of interest ("Manageable Conflicts") and prevent certain other types of conflicts of interest ("Prohibited Conflicts"). Additional detail pertaining to conflicts of interest and EJR's approach to managing/avoiding them is found in the Conflicts and Compliance Manual. Manageable Conflicts that are not in practice being properly managed and Prohibited Conflicts that are not being prevented are reportable events.

Policy Against Retaliation

EJR is committed to ensuring that all of our people feel safe and protected when reporting issues. The firm prohibits and will not tolerate any kind of retaliation or retribution for reports or complaints (internally or via the independent helpline) regarding firm misconduct or the misconduct of others that were made in good faith. Open communication of issues and concerns by all Associated Persons without fear of retribution or retaliation is vital to the continued success of the Firm. Unless the Firm's management learns of a problem, the Firm cannot deal with it. Concealing improper conduct often compounds the problem and may delay or hamper responses that could prevent or mitigate actual damage.

Measures to be Undertaken in the Event of a Material Breach

The DCO is primarily responsibility for monitoring the Firm's compliance with its policies and procedures. This Code of Conduct details prohibited conflicts of interest, identified conflicts and many other areas of compliance concern. All Associated Persons are required to notify the DCO whenever they become aware of a possible violation of a policy or procedure. The DCO will, upon discovering a possible violation or having been provided with evidence that indicates a possible violation, immediately assess the available evidence and document the results of the investigation. In the case of

serious violations, the CEO, Independent Board members and, if appropriate, counsel, maybe contacted by the DCO and provided with the details of the violation. If the violation is indeed a material violation, the DCO will consider whether the appropriate regulatory bodies must be notified.

Consequences of Violating the Code

If you are an Associated Person (other than an independent contractor), this Code forms part of the terms and conditions of your employment at the Firm; if you are an independent contractor this Code forms part of your agreement to provide services to the Firm. All Associated Persons are expected to cooperate in internal investigations of allegations of violations of the Code, and actual violations may subject you to the full range of disciplinary action by the Firm, including termination. The Firm may also report certain activities to its regulators, which could give rise to regulatory or criminal investigations. The penalties for regulatory and criminal violations may include significant fines, permanent bar from employment in the securities industry and, for criminal violations, imprisonment.

Attestation, Waivers, Amendments and Contact Information

Associated Persons are required to attest their knowledge of, and compliance with, the above-mentioned policies and procedures. Waivers and amendments to this Code, and any specific policy exemptions, must be approved and documented by the DCO. It is your responsibility to be familiar with the Code. If you have any questions regarding the Firm's Code of Conduct, the contact information is:

By mail to: Egan-Jones Ratings Company
Attn: Compliance Department
61 Haverford Station Rd Haverford, PA
19041 Compliance@egan-jones.com

Handling of Confidential Information and Material Nonpublic Information (17g-4)
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

During the course of the Firm's business activities, analytical staff and other Associated Persons may attend meetings and discussions with issuers, arrangers, clients or potential clients to discuss analytical components of products or methodologies, or be exposed to documents (financial and otherwise) that are not generally in the public domain. Thus, there is a possibility that the

Firm and/or its Associated Persons may be exposed to material, non-public information (MNPI) and/or confidential information (collectively "MNPI"). MNPI may be obtained in various ways, including verbally, through physical documentation, and in electronic form. Pursuant to Rule 17g-4 and section 15(E)(g) of the Exchange Act, the Firm is required to have policies tailored to the nature of its business which are reasonably designed to address the handling of MNPI by the NRSRO and/or its Associated Persons and prevent the:

- The inappropriate dissemination within and outside the NRSRO of MNPI obtained in connection with the performance of credit rating services;

- A person within the NRSRO from purchasing, selling, or otherwise benefiting from any transaction in securities or money market instruments when the person is aware of MNPI obtained in connection with the performance of credit rating services that affects the securities or money market instruments; and

- The inappropriate dissemination within and outside the NRSRO of a pending credit rating action before issuing the credit rating on the Internet or through another readily accessible means.

Specifically, section 15(E)(g)(1) of the Exchange Act states: "Each nationally recognized statistical rating organization shall establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of the business of such nationally recognized statistical rating organization, to prevent the misuse in violation of this title, or the rules or regulations hereunder, of material, nonpublic information by such nationally recognized statistical rating organization or any person associated with such nationally recognized statistical rating organization."

MNPI will be sequestered and may not be shared with members of the Firm who are not required to know. The Firm's Employees are prohibited from using, propagating, tipping, or in any other way passing MNPI on to any other persons other than the Firm's Compliance or Legal personnel. The Firm's Compliance Department will, on an at least annual basis, review the Firm's operations to identify potential exposure to MNPI and to review policies to address identified and emerging conflicts. At no time may the Firm or any member of the Firm discuss or disclose such information to third parties other than in accordance with the Firm's Code of Conduct or perform any personal securities or money market transactions while in possession of MNPI with respect to such security.

Pending Credit Rating Action

Confidential information includes information concerning a pending rating or rating-related action prior to the announcement of that rating or rating-related action. In connection with issuing ratings for transactions, the Ratings Group may not disclose or discuss potential or pending rating actions with external parties without appropriate permission from the Compliance Department, unless and until that information has been publicly disclosed.

In the event that an employee misuses or passes on MNPI, or in the event that personnel from external parties receive non-public information about potential or pending rating actions, the Compliance Department in consultation with EJR's legal department as needed, will investigate the matter fully, assess the cause and seriousness of such infraction, will determine an appropriate response and consider whether to implement measures designed to prevent misuse of the information to the extent appropriate under the circumstances, and will document all findings, responses and such consideration.

At least annually, the firm will conduct a compliance meeting / training session during which issues, procedures and policies related to the possession and use of MNPI will be discussed.

The Firm's information security procedures are intended to provide effective control to prevent misuse of material, nonpublic information across all information technology systems. The Firm's employees are assigned unique Windows and email login credentials, and appropriate user's group and access rights based on their roles and responsibilities. After exiting EJR, the former employees' email accounts and other accesses rights shall be disabled promptly, and if applicable, incoming messages shall be

redirected to the appropriate current employees. Current employees should not be able to use the former employees' email address for sending messages.

Separation Between Ratings and Marketing
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

The Firm's Ratings Group is separated from the Sales and Marketing areas and isolated from information regarding fees. Analysts are prohibited from inquiring about fees pertaining to EJR's credit ratings. Analysts are prohibited from determining a credit rating in a manner inconsistent with EJR's policies, procedures, methodologies and models for determining credit ratings

Electronic segregation- EJR's analytical staff members ("Rating" staff) are required to store the following written and electronic records and communications ("Documents") in a manner that is not accessible to EJR's sales and marketing staff members ("Marketing" staff):

- Documents containing EJR's proprietary credit rating analysis
- Documents containing EJR's proprietary model inputs and/or outputs
- Documents containing RRC recommendations
- Documents containing RRC decisions

Marketing staff are required to store the following written and electronic communications in a manner that is not accessible to Ratings staff:

- Contracts and statements of work (SOW) with credit ratings clients
- Documents containing sales/marketing strategy
- Documents containing fees and/or contract terms

Physical segregation in EJR office locations- EJR maintains separate workspaces in its Haverford and New York offices which are dedicated Ratings and non-Ratings staff. While communication between Ratings and Marketing roles is often necessary, Ratings staff are not permitted to become involved in any sales or marketing activities. Likewise, Marketing staff are not permitted to become involved in or attempt to influence any analytical activities. As a general rule, communications between Ratings and Marketing staff should take place by phone, e-mail, or in a conference room outside of workspaces that are exclusively dedicated to one role. Limited exceptions to the above may be permitted subject to written pre-approval from the DCO. The DCO will centrally retain records of any limited exceptions, along with the rationale for such eFirmxceptions.

Remote work considerations- Staff working remotely must maintain at all times a clean desk policy in their home office workspace. This helps EJR to safeguard client confidential information and material nonpublic information.

Escalation to Compliance- In the event that Ratings or Marketing staff identify any concerns regarding the effectiveness of EJR's physical or electronic segregation protocols, they should immediately contact the Compliance Department.

Legitimate Business Need to Know- EJR is obligated to safeguard client confidential information and material nonpublic information (MNPI) in accordance with legitimate business purpose. Individuals who do not have a legitimate business need to know client confidential information and/or MNPI should not receive such information via e-mail or other means of written, electronic, or oral communication.

Members of the Ratings Group are prohibited from emailing or otherwise sharing information regarding unissued and final credit ratings reviews and non-public credit ratings reports or company-related MNPI with anyone not directly involved in reviewing the credit rating itself. Individuals directly involved in reviewing the credit rating typically include—with respect to the specific credit rating – the primary analyst, the reviewing analyst, personnel responsible for collecting/inputting ratings-related data and information into EJRs analytical models and related formats, personnel responsible for performing analytical file or ratings quality reviews, and rating committee members (i.e., those who are attending the relevant rating committee for voting or training purposes).

Pursuant to Rule 17g-5(c)(6), a person who participates in negotiating, discussing, or arranging rating fees shall not participate in determining credit ratings, or developing or approving procedures or methodologies used for determining credit ratings, including qualitative and quantitative models.

Importantly, pursuant to Rule 17g-5(c)(8), no Firm Employees who participate in determining or monitoring credit ratings, or developing or approving procedures or methodologies used for determining credit ratings, including qualitative and quantitative models, may also: (i) Participate in sales or marketing of an EJR, EJP, or other ancillary product or services (including the determination and negotiation of fees for ratings, proxy, and other ancillary services); or (ii) be influenced by sales or marketing considerations. The sales staff is responsible for negotiating, discussing, and arranging fees. The responsibility of fee determination and negotiation is specifically segregated away from the Ratings so that the ratings analysts are not exposed and possibly influenced by the sales and marketing considerations.

Employees must also ensure to abide the above rules while they attend conferences, professional events, and other similar settings.

The sales and marketing department should not include commercial terms in any e-mail correspondence with ratings staff and should instruct clients of such limitation.

In the event that analysts become aware of any fees, they shall report to their supervisor (without forwarding the fee information to other analyst) and Compliance Department immediately. Unless the Compliance Department determines that Analytical staff who have come into contact with fee information have not: (a) participated in and (b) been influenced by sales or marketing considerations, they shall be removed from the process of rating that issuer or follow the direction given by the Compliance Department.

In the event that a sales/marketing employee is exposed to rating information before the rating is finalized, the employee shall promptly report such fact to the Compliance Department and follow their guidance. The Compliance Department shall review the cause of the event and provide prevention if possible.

Separation Between Compliance and Marketing
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

Compliance personnel are prohibited from acting in any marketing capacity.

Procedure for Internal Role Changes
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

Scope of this Procedure- This procedure provides guidance to staff members when changing roles internally.

Definitions

Analytical Role- The staff member participates in performing credit rating analysis, voting in a rating committee, or developing or approving models, procedures or methodologies used to determine credit ratings. An Analytical staff member may never participate in sales or marketing activities.

Analytical Activities- Analytical Activities means: (i) participation in determining or approving credit ratings, as well as (ii) participation in developing or approving models, methodologies or procedures that are used to determine credit ratings.

Commercial Role- The staff member's primary responsibilities entail the day-to-day performance (either as an individual contributor or as a department manager) of sales and / or marketing activities. A Commercial staff member may never participate in Analytical Activities.

General Management Role- The staff member's primary responsibilities entail the day-to-day performance (either as an individual contributor or as a department manager) of functions such as operations, business strategy, IT, HR, compliance, legal, risk management or similar roles. A General Management staff member may directly or indirectly supervise staff members in a Commercial Role or Analytical Role, though not in the capacity of a department head. A General Management staff member may participate from time to time in sales and marketing activities. A General Management staff member may never participate in Analytical Activities.

Cooling Off Period- A period of time during which a staff member may not perform some or all of the responsibilities associated with their new role. A Cooling Off Period lasts for two months from the date the staff member begins their new role. A Cooling Off Period is not required in all instances. In addition, the DCO is empowered to make certain exceptions to a Cooling Off Period, provided that enhanced compliance monitoring is performed and documented in all cases where exceptions are made. See below for further detail.

Changing Roles

Transitioning from a Commercial Role or a General Management Role to an Analytical Role- Staff members shall observe a Cooling Off Period pertaining to the following activities: voting in a rating committee; developing models, procedures and methodologies used to determine credit ratings; and approving models, procedures and methodologies used to determine credit ratings. Staff members may perform credit rating analysis provided they do not act as a Primary Analyst during the Cooling Off Period. During a Cooling Off Period, staff members may attend internal meetings pertaining to models, procedures and methodologies used to determine credit ratings in order to facilitate learning / getting up to speed on analytical matters. Effective Date: February 23, 2021

Transitioning from an Analytical Role to either a Commercial Role or a General Management Role- Staff members shall observe a Cooling Off Period pertaining to the marketing or selling of credit ratings to any Person (as defined in the federal securities laws) for whom the staff member either voted in a rating committee or acted as a Primary Analyst during the preceding six months.

Transitioning within or between General Management Roles and Commercial Roles- No Cooling Off Period is required.

Other Matters to Consider

Network Access- Staff members are accountable for ensuring that their network appropriately reflects their role on the day they begin their new role. Consultations with Compliance should take place prior to effective date of any new role, as necessary.

Training- Staff members are accountable for ensuring they complete any required training (as determined by their manager) within one month of beginning a new role.

Separation Between Ratings and Proxy
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

Egan-Jones Proxy Services ("EJP") provides research, recommendations, voting, and voting record keeping services on various shareholder proxy voting matters. The service includes an evaluation of the various agenda items in the proxy statements, recommended voting action, and an overall rating of the firms' corporate governance. In addition, EJP provides a web-based interface to enable clients to access reports prior to the voting date which are archived thereafter for up to five years. EJP and EJR personnel do not have access to each other's client websites, client holdings, draft reports, and other aspects related to the issuance of reports for each business. EJP personnel may not be involved in the generation of EJR ratings reports and EJR personnel may not be involved in the generation of EJP reports. The Firm restricts rating analysts from initiating meetings with current and prospective proxy clients, and they are also restricted from exposure to sales and marketing efforts. The Firm's executives who might be involved in the rating review process must also comply with such rules even though they are allowed to communicate general Firm support to current and prospective clients.

EJP and EJR personnel must remain separate from each other's social media websites. For example, no tweets or re-tweets are permitted from EJP to EJR, or vice-versa involving proxy positions, voting, client information, and any other information that may influence the independence of ratings. Access to any social media websites shall be approved by the Compliance Department. The Compliance Department monitors social media activities in accordance with procedures set out in the Compliance Operating Guide section 40.

Personal Securities Transactions and Holdings
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

Detailed guidance pertaining to personal securities transactions and holdings is provided in EJR's Code Conduct on page 15. These standards and controls help the firm comply with regulatory expectations pertaining to prohibited conflicts of interest that might arise in connection with analysts' (or their direct family

members') personal securities holdings, as well as preventing the misuse of material nonpublic information. EJR's personal securities policy is designed to address potential conflicts of interest in cases where its

Associated Persons have ownership positions in issuers the Firm does business with. The policy generally only allows for the ownership or trading of mutual funds, ETFs and the existence of blind trusts and similar investment vehicles managed by a third-party, where the Associated Person has no direct or indirect influence or control over the trust or account ("Third-Party Accounts"). Any waivers and exemptions shall be granted by the Compliance Department. Monitoring of personal securities transactions and holdings is performed by EJR's Compliance Department. Compliance Department standards for monitoring compliance with EJR's Personal Securities Transactions and Holdings Policy are contained in the Compliance Operating Guide section 33

Outside Business Activity Reviews
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

The Compliance Department performs reviews of Associated Persons' outside business activities in order to identify and address any potential conflicts with respect to EJR business activities. The Outside Business Activities Disclosure Form is located in the Conflicts and Compliance Manual Appendix on page 7. Associated Persons provide certifications with respect to their outside business activities when completing the

annual Compliance Response Sheet questionnaire. Board members provide certifications with respect to their outside business activities when annually attesting to the Board Code of Conduct.

Outside business activities are defined as any activity undertaken by an Associated Persons or Board member involving a business enterprise unrelated to the Firm or involving an entity which might be rated by the Firm, including any employment, paid consulting activities or serving on a company board. Excluded from this definition are activities with civic, religious, academic, non-profit, and other similar enterprises. The firm requires Associated Persons and Board members to disclose their outside business activities during the on-boarding process. Any new outside business activities must be pre-approved by the Compliance Department.

Ratings analysts specifically are not permitted to have outside business activities which conflict with the issuance of ratings.

EJR's Compliance Department performs reviews of outside business activities in accordance with procedures set out in the Compliance Operating Guide sections 32 and 19.

OUTSIDE BUSINESS ACTIVITIES DISCLOSURE FORM

Egan-Jones Ratings Company ("EJR") defines outside business activities as any activity involving a business enterprise or an entity which might be rated or covered by EJR. Civic, religious, academic, non-profit, and other similar enterprises are excluded from the definition.

Outside business activities by employee, independent contractor, or director (collectively an "Associated Person") may present a potential conflict of interest, and are required to be disclosed. Ratings analysts are not permitted to have outside business activities which conflict with the issuance of ratings.

All Associated Persons are required to disclose their outside business activities upon initial employment (or assignment for directors), annually thereafter, and when there is a change in outside business activity status.

I have outside business activities: YES ☐ NO ☐

If YES, please list and provide requested information for all outside business activities:

Name of Outside Activity / Entity	Role in Outside Activity	Are You Compensated?	Does Outside Activity/Entity Know Your EJR Status?

Print Name:

Signature:

Date:

Standard for Shared E-Mail Addresses
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

Background and scope- NRSROs are subject to laws and regulations pertaining to (among other things): (i) safeguarding client confidential information; and (ii) the separation of roles. This policy and procedure seeks to formalize standards governing the creation and maintenance of shared e-mail addresses that are intended to be utilized with or by external parties for either analytical purposes or sales and marketing purposes. This policy is not designed to address e-mail addresses used by external parties for other purposes (e.g., complaints@egan-jones.com) or e-mail addresses designed for internal communications (e.g., employees@egan-jones.com).

Analytical communications- Shared e-mail addresses that are utilized with external parties to facilitate credit rating analysis may include only the following types of roles: Analytical and Operations. For each non-Analytical individual on a shared Analytical e-mail address, EJR's Compliance Department will retain documentation pertaining to their legitimate business need to receive the intended client communications and consideration of any conflicts of interest.

Sales and Marketing communications- Shared e-mail addresses that are utilized with external parties to

facilitate sales and marketing objectives may include only the following types of roles: Sales, Marketing and Operations. For each non-Sales and Marketing individual on a shared Sales and Marketing e-mail address, EJR's Compliance Department will retain documentation pertaining to their legitimate business need to receive the intended client communications and consideration of any conflicts of interest.

Audit trail- EJR's IT Department is accountable for retaining an audit trail of each individual added to / dropped from a shared e-mail address that is utilized with external parties.
DCO Exceptions- The DCO is authorized to grant access to other individuals on a case-by-case basis, provided the DCO confirms and documents: (i) that the individual has a legitimate business purpose for obtaining access; and (ii) that Sales/Marketing and Analytical roles will not be on the same shared e-mail address.

Standards Governing Approved as well as Off-Channel Communications Platform
(EJR Conflicts and Compliance Manual Effective 06/30/2023)

As a regulated credit rating agency, Egan-Jones is required to make and/or retain certain types of records, including many types of written communications.

Where written electronic communications are concerned, approved communications platforms are limited to associated persons' electronic communications accounts provided by EJR's IT Department. Approved communications platforms are presently limited to corporate e-mail via Microsoft Outlook, messaging via Microsoft Teams, messaging via EJR's Client Portal, and EJR's official social media accounts.

Internal and external communications for EJR business purposes which take place on unapproved communications platforms ("Off-channel Communications") are prohibited, subject to limited exceptions discussed below. Off-channel communications may include, but are not necessarily limited to, SMS/texting services; encrypted messaging services such as "WhatsApp," "Signal," or "Telegram"; personal e-mail messages; and non-official social media accounts.

As discussed above, there are limited exceptions where Off-channel Communications may take place. These exceptions include simple coordination of legally, ethically, or regulatorily-permissible actions. Examples of limited exceptions can include the use of text messages to coordinate a time to meet or speak. When sending such text messages, associated persons must refrain from discussing specific business matters that relate to initiating, determining, or monitoring a credit rating.

Types of Credit Ratings Policy
(Types of Credit Ratings Policy Effective 1/10/2022)

Contents

I. Private Credit Ratings
II. Public Credit Ratings
III. Additional Guidance Pertaining to Credit Rating Dissemination
IV. Conversions Between Types of Credit Ratings

***

I. Private Credit Ratings

Private credit ratings are deemed to be solicited credit ratings. A private credit rating is a credit rating that is disseminated to the requestor of the credit rating. As applicable, a private credit rating may

also be disseminated to a limited number of parties/agents authorized by the requestor of the credit rating. (For this purpose, a request to post a rating on Bloomberg or similar service or to provide a rating to the NAIC or similar supervisory authority shall not alter the classification as a private credit rating.)

Whether a credit rating is to be a private or public credit rating shall be at the discretion of the client (assuming the client's request is consistent with EJR's policies and procedures). In the absence of clear direction from the client, a credit rating shall be deemed to be a private credit rating.

II. Public Credit Ratings

Public credit ratings that are determined without client/issuer participation are deemed to be unsolicited credit ratings. All other public credit ratings are deemed to be solicited credit ratings.

Subscription credit ratings- Subscription credit ratings are generally unsolicited credit ratings. Subscription credit ratings are disseminated via EJR's subscription platform and are generally determined using publicly available information.

Full dissemination credit ratings- In cases where EJR makes use of non-public/confidential information in determining a public credit rating, the rating shall be disseminated on EJR's free public website. Such ratings may not be disseminated exclusively on EJR's subscription platform. However, it is permissible to also post a full dissemination credit rating to EJR's subscription platform after it has been posted to EJR's free public website.

III. Additional Guidance Pertaining to Credit Rating Dissemination

Pre-Publication Notices

For issuer-paid, full dissemination credit rating actions (new, surveillance, and conversions) a , EJR's analytical team shall disseminate to the issuer a draft rating report for the purposes of: (i) confirming there are no factual inaccuracies in the report; and (ii) confirming that EJR is not inadvertently disseminating confidential information. (Withdrawals that are not the result of credit rating analysis do not require a pre-publication notice.)

For investor-paid (or other client, non-issuer-paid), full dissemination credit rating actions (new, surveillance, and conversions), EJR's analytical team shall disseminate to the client and to the issuer a draft rating report for the purposes of each such party: (i) confirming there are no factual inaccuracies in the report; and (ii) confirming that EJR is not inadvertently disseminating confidential

information. (Withdrawals that are not the result of credit rating analysis do not require a pre-publication notice.)

The requirements of this section shall be satisfied if a party is provided with a near-final draft rating report for review. This section does not require that every draft or subsequent revised draft be made available for review.

17g-7 Reports

It is EJR's policy to disseminate directly or to make available via internet link a disclosure report in the form required pursuant to Rule 17g-7(a) under the Securities Exchange Act of 1934, as amended (each, a "17g-7 Report") for each credit rating that is disseminated.

For private credit ratings and public subscription credit ratings, the 17g-7 report is included at the end of the rating report.

For full dissemination public credit ratings, a 17g-7 Report may be included at the end of the rating report. In certain other cases in which EJR publishes a brief rating summary in lieu of a full rating report, the 17g-7 Report shall be included (directly or via a link) as a standalone document. In such cases, Analytical staff must take care to ensure that the 17g-7 Report is sufficiently detailed (as the 17g-7 Report may not reference information contained within the full rating report).

Social Media and Press Releases

EJR may choose to make certain public full dissemination credit rating announcements via social media or press release after the credit rating has been posted to EJR's free public website. In such cases, EJR shall include in the announcement a link to the section of EJR's free public website that contains the applicable 17g-7 Report.

IV. Conversions Between Types of Credit Ratings

Upon client request or for business, compliance or other internal reasons, EJR may, in its own discretion, process a conversion between certain types of credit ratings. EJR will generally not maintain both public and private credit ratings on the same company or the same instrument at the same time. The conversion scenarios detailed below are permissible. Certain other conversion scenarios may also be permissible, subject to written pre-approval from both Legal and Compliance.

Converting a Public Subscription Credit Rating to a Private Credit Rating- If EJR receives an external request to provide a private credit rating on a credit which is presently being rated on the subscription side based solely on public information, the recipient of the request shall notify Compliance of the request and the circumstances of the request. While Compliance pre-approval is not needed to proceed, Compliance shall nonetheless consider the facts and circumstances of the request, including the reason for such request and the nature of the requesting party, and any potential conflicts of interest presented by such request and, if appropriate, place a hold on the conversion while matters are being evaluated. Compliance may consult with Legal, General Management and other departments. In addition, if circumstances arise such that business, compliance or other internal

reasons are deemed to necessitate that a rating no longer be maintained as a public rating, Compliance may determine that such rating be converted to a private credit rating. Any

determinations will be made in the sole and absolute discretion of EJR. Absent any internal decision to not proceed, the RRC will undertake the following steps:

Step 1: Prior to issuance of a private credit rating, staff shall cause a withdrawal notification to be publicly disseminated for the credit. For a rating which is a subscription rating, a notice included on the subscription section of EJR's website shall satisfy the dissemination requirement.

Step 2: The request for a private credit rating shall be considered a new ratings request and the Analytical team shall follow applicable policies and procedures with respect to such new rating, including RRC assignment of such private credit rating.

Step 3: The Analytical team shall follow applicable policies and procedures with respect to dissemination of the newly-assigned private credit rating.

Converting a Private Credit Rating to a Public Full Dissemination Credit Rating- A request to convert a private credit rating to a public full dissemination credit rating may be received by a client from time to time. (For this purpose, a request to post a rating on Bloomberg or similar service or to provide a rating to the NAIC or similar supervisory authority shall not be considered a request to convert a rating to a public credit rating.) Upon receipt of such client request, the recipient of the request shall notify Compliance of the request and the circumstances of the request. While Compliance pre-approval is not needed to proceed, Compliance shall nonetheless consider the facts and circumstances of the request, including the reason for such request and the nature of the requesting party, and any potential conflicts of interest presented by such request and, if appropriate, place a hold on the conversion while matters are being evaluated. Compliance may consult with Legal, General Management and other departments. Any determinations will be made in the sole and absolute discretion of EJR. Absent any internal decision to not proceed, the RRC will undertake the following steps:

Step 1: The analytical team shall send a written notification (which may be by e-mail) to the client confirming that the rating will be converted to a public credit rating and the expected approximate date of such conversion. The notification should convey that EJR will disseminate the credit rating, along with all surveillance updates, on its free public website.

Step 2: Where the most recent rating action was issued 90 or fewer days ago, the request for a public credit rating shall not be considered a new ratings request; procedures set forth above in Section III shall be followed with respect to the dissemination of a public, full-dissemination credit rating. Where the most recent rating action was issued 91 or more days ago, the request for a public rating action shall be treated as a new rating request; the analytical team shall follow applicable analytical procedures pertaining to new public credit ratings, as well as procedures set forth above in Section III with respect to a public, full-dissemination credit rating.

Information Security Policy
(Information Security Policy Effective 12/03/2021)

TABLE OF CONTENTS

Introduction 3
Purpose 3
Scope 3
Contact Us 3
Roles and Areas of Responsibility 4
System Administrator 4
User 5
Consultants and Contractual Partners 6
Information Security During Employment Process 7
Prior to Employment 7
During Employment 7
Termination or Change of Employment 7
Internet Usage Policy 8
Policy 8
Best Practices 8
Email Policy 9
Policy 9
Best Practices 9
Intranet & Internal Web Application Policy 11
Policy 11
Best Practices 11
Mobile Device Policy 12
Policy 12
Best Practices 12
Password Policy 13
Policy 13
Best Practices 13
Anti-Virus Policy 14
Policy 14
Best Practices 14

Windows and Workstation Policy 15
Policy 15
Best Practices 15
Remote Access Policy 16
Policy 16
Wireless Internet (Wi-Fi) Policy 17
Policy 17
Best Practices 17
Social Media 18
Policy 18
Best Practices 18
Data Protection & Retention Policy 19
Policy 19
Cybersecurity Breach Response Procedures 20
Disciplinary Consequences 20
Appendix A – Data Classification 21
Appendix B – Important Contacts 22

Introduction

This document is developed and maintained by the Egan-Jones Information Technology ("IT") department. The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of Egan-Jones Ratings Company ("EJR"). Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for EJR to recover.
The Information Security policy outlines EJR's approach to information security management.

Purpose

The purpose of this policy is to provide instructions on measures that must be taken by all EJR and its affiliates' employees to help achieve effective information security and best practices and to protect Material Non-Public Information ("MNPI") and Cybersecurity that are required by EJR, regulators, and Securities Law.

Scope

This policy applies to all EJR and its affiliates' employees, vendors, and all other third parties who interact with information held by EJR and the information systems used to store and process it. This includes, but is not limited to, workstations, telephone networks, mobile devices, remote desktop client applications, file transfer protocol ("FTP") client applications, and any other software used to connect to the EJR network.

Contact Us

IT department can be reached by phone at (610) 642-2411 extension 1400 or by email at it@egan-jones.com for any comments and questions you may have.

Roles and Areas of Responsibility

System Administrator

System administrators are persons (within the EJR IT department) administrating EJR's information systems. Their basic responsibilities are maintaining the firm's systems, safeguarding all confidential data (including client and employee data), and preventing external sources from gaining access to the firm's network. The following are the rest of the responsibilities of a system administrator:

1. Report all incidents to Compliance. All cybersecurity incidents must be reported to the EJR Compliance department. EJR is regulated by the U.S. Securities and Exchange Commission ("SEC"). So, the firm must follow all of the rules and procedures set by the SEC.
2. Apply all security updates. The IT department is responsible for maintaining all of the computers in the network. Security updates are scheduled to be applied on every computer within the network only a weekly basis (if available). This includes, but not limited to, anti-virus software, anti-virus definition, Windows security, and all other software updates.
3. Inventory all equipment. System administrators must perform a monthly inventory of all office equipment including, but not limited to, hard drives, computers (old and new), printers, USB drives, printers, and external optical drives.
4. Log all network access. The IT department must maintain a log of all network activities including Windows logins, EJR website logins, and drive exchange transactions (part of the disaster recovery process).
5. Maintain data backups. As part of the network disaster recovery plan, the IT department must

ensure that daily, weekly, and monthly backups are fully functional. This includes data from all of EJR web properties (on Amazon AWS), workstations, and file server. (See EJR Disaster Recovery Plan for more information).

6. Prevent data loss. The IT department must ensure that all internal data stays within the firm, especially clients' personal identifiable information ("PII"). Hard drives from retired workstations must be removed and backed up immediately. All memory modules must be removed as well. Any failed hard drives and memory modules must be physically destroyed prior to disposal.
7. Execute network vulnerability tests. The IT department must conduct a network vulnerability test on the internal network and EJ's web properties at least once a year. The external tests should be done by a private firm that specializes in cybersecurity.
8. Test disaster recovery plan. The IT department must test the network disaster plan, at least, once a year. Core functionalities (such as publishing new reports and FTP connectivity) must be operational during this test.
9. Execute disaster recovery plan. In an event of a disaster, the IT department must ensure that the firm's core functionality is fully operational within 24 hours. *(See EJR Disaster Recovery Plan for more information)*
10. Run anti-virus scans. The IT department must ensure that the anti-virus software is running properly on each workstation. A full virus scan is scheduled to run once a week on each workstation. The IT department must also ensure that real-time scanning is active on every workstation
11. Train EJR employees. The IT department must train all of the EJR employees on cybersecurity risks. Training can be done in person, via email, or on the phone. The IT department must make sure that all employees understand all of the IT policies and procedures.
12. Respond to cybersecurity events. In an event of a security breach, the IT department must respond quickly. This includes, but not limited to, notifying the Compliance department, patching the security hole (if any), notifying affected clients (if any), contacting law enforcements, and writing up an incident report. *(See Cybersecurity Breach Response Procedures below for more information)*
13. Update policy annually. The IT policy should be reviewed and updated, at least, once a year.

User

Users are all employees within the firm. The following are the users' responsibilities:

1. Handle all information with care. All EJR employees are responsible for the security of all data which may come to them in whatever format. This includes, but not limited to, PDF, MS Word documents, Excel documents, picture files (JPG, PNG, GIF, PSD, etc.), and raw text files.
2. Take care of your equipment. All EJR employees are expected to take proper care of their workstations and/or laptops. Employees must not abuse their keyboard, mice, or any other peripherals that belongs to the firm.
3. Protect your workstation. All EJR should lock their workstations and/or laptops when they are away from their desk. Even though the network policy will lock the computers automatically after fifteen (15) minutes, it is highly recommended that all employees lock their computers manually

immediately when they are leaving their desk.

4. Internet access. All users that are logged into the EJR network should use the internet primarily to perform their work-related duties. Do not download any unapproved applications. Downloading an unapproved application may harm your workstation. Non-IT employees should not give the firm's Wi-Fi access to EJR guests without approval from the IT department.

5. Stay away from social media. Unless it's work-related, you should not log into any social media website (i.e. Facebook, Twitter, and LinkedIn) while at work. Keeping yourself distant from these sites will minimize the risk of exposing confidential information.
6. No removable storage devices allowed. The EJR network policy prohibits all EJR employees from accessing removable storage devices such as a USB thumb drive. If any employee need temporarily access to their removable storage device, a written request must be sent to the information technology ("IT") department from their supervisor.
7. Do not use another employee's email. *(See Email Policy on page 9).*
8. Do not use your cell phone while at your desk. *EJR employees should not use their personal cell phone or mobile devices for an expended period period while sitting at their desk. Users are encouraged to use their cellphones outside of the office.*
9. Report information security issues immediately. If any EJR employee is aware of any information security incident, they must report the incident to the IT department at once. The IT department can be reached by phone at (844) 495-5244 extension 1400 or by email at it@egan-jones.com.

Consultants and Contractual Partners

Consultants and contractual partners are persons or companies that the firm may hire for a specific purpose. The role and responsibilities of a contractor or consultant is based on the service agreement. They are also required to follow the firm's policies and procedures.

Information Security During Employment Process

Prior to Employment

- A background check is to be carried out of all appointees to positions at EJR according to relevant laws and regulations.
- A confidentiality agreement should be signed by the employees, contractors, or others who may gain access to sensitive and/or internal information.

During Employment

- The IT policies and regulations should be reviewed regularly with all users and new hires.
- Employees must follow all of the policies described in this document.
- Employees must make all attempts to prevent damage to their workstations.

Termination or Change of Employment

- A system administrator must change the password of the former employee's email account immediately so that they would not be able to send new emails.
- Emails will be forwarded to the respective department manager or appropriate person.
- The department manager or system administrator will need to setup an autoresponder to inform people that the employee is no longer with the firm.
- All other accounts (such as Windows and the firm's web properties) must be deactivated immediately.
- All IT assets (such as laptops or cell phones) that were given to the employee must be returned in working condition.

Internet Usage Policy

The firm has firewall rules in-place to restrict certain websites from being accessed within the network.

This policy applies to internal, cellular, and all open Wi-Fi networks.

Policy

1. Employees must not visit any inappropriate websites during work (i.e. gambling, pornography, torrent, pirated video or software forums, phishing, hacking, drugs, IRC chats, etc.).
2. Employees are prohibited from accessing all email service provider's website (i.e. Gmail, Yahoo Mail, Outlook, etc.) except the firm's own web mail service.
3. Employees working remotely may transmit data using SFTP (Secure File Transfer Protocol) if they are work-related. Downloaded files should be saved in a work-only folder on the employee's computer.
4. Employees are prohibited from transmitting data to/from their personal FTP site(s), file- sharing websites (i.e. Mega, Dropbox, Box, Google Drive, etc.), and personal websites/blogs without IT's approval.
5. Employees are prohibited from signing in and uploading data to any file-sharing website that has not been approved by the IT Department.
6. Employees must not use the firm's network to stream videos for an extended period of time (i.e. more than 10 mins).

Best Practices

1. Use the internet for work-related activities only.
2. Do not go to any NSFW ("not safe for work") websites.
3. Get permission from the IT department if you need to access a restricted website for a work-related project.
4. Be careful of what you download from file-sharing websites (even if it's shared by a client). Consult the IT department if you are unsure if it is safe or not.

Email Policy

The IT department supports all versions of Microsoft Outlook (2010 and up) email clients. Webmail access is also available for backup and remote users.

The account will be automatically locked after five (5) consecutive login failures. The user must contact the IT department it@egan-jones.com to have their password reset if their account has been locked.

Policy

1. Employees must use their company email address (i.e. egan-jones.com or ejproxy.com) for all business-related activities.
2. Employees must not transmit data between their personal accounts (i.e. Gmail, Yahoo, Hotmail, etc.) and work email for any reason.
3. Employees should not download any attachments from unknown senders.
4. Employees should not use another employee's email account to send out emails on their (the other employee) behalf for any reason.
5. Employees should never reply to an email (from someone outside of the firm) with their personal or financial information.
6. Employees should not respond to any emails containing the word "spam" in the subject.
7. Email must be archived for, at least, 3 years.
8. The IT department must change the user's password immediately after they exit the firm. (See *Termination or Change of Employment* under *Information Security During Employment Process*)

Best Practices

- Employees are encouraged to be professional at all times when composing any email (especially to clients).
- Do not log into another user's computer to check their emails for any reason.
- Remember that emails are not considered private. Once an email has been sent out to the recipient, it can be viewed by other people at the receiving end.
- Employees should not respond to emails from unknown senders.
- Use the spellcheck tool before sending out an email.
- Check and double check for any possible errors, i.e., the recipient's email address.

- Do not send any emails with file attachments totaling over 5MB in size. Most of the time, the email will get rejected by the recipient's email server. A simple solution is to break up the attachments into separate emails.
- The bottom of the email message should include your signature.
- Do not include your personal phone number or personal email address in your email signature.
- Do not include any social media links in your email signature without getting it approved by the Compliance department first.
- Watch out for "phishing" emails. Phishing is the activity of defrauding an online account holder of financial information by posing as a legitimate company. For example, the body of a phishing email may contain a phrase like, "Your bank account information is out of date. Click here to update it."
- Do not send email containing any of your personal information (such as social security number and bank account information) to anyone.
- Before clicking on a link in the body of an email, hover your mouse pointer over it first and see if the URL (link) contains the sender's domain name in it. If it doesn't, it's most-likely not a legitimate link.
- Consult the firm's IT department if you are unsure if an email is legitimate.

Intranet & Internal Web Application Policy

Policy

- Employees must never use any of EJR's internal web properties/applications in a public setting (i.e. Starbucks).
- Employees must not share their login credentials with anyone.
- Employees must not share the web address (or URL) of the web application to anyone outside the firm.
- Employees must not share screenshots, files, or anything related to the web application with anyone outside the firm or outside entities such as social media.
- Employees should not attempt to login as another user.

Best Practices

- Always access the firm's intranet/internal web application from a private location (i.e. your office).
- Treat all data within the web application as they were your own – keep them private.
- Make sure your internet connection is secure (i.e. do not connect to an open WiFi network).
- Always log out of the application when you are done working.
- Keep your login credentials private.

Mobile Device Policy

Policy

- Employees must not take pictures or record video or audio while in the office.
- Employees must not transfer data between their work computer and personal mobile device(s).
- Employees must not give out their personal cell phone number to clients.
- Employees must set their mobile device(s) on silence mode while working in the office.
- Personal mobile devices are prohibited from connecting to the firm's Wi-Fi network.
- Employees must not download any illegal apps or pirated music or videos using a company-issued mobile device.
- Only company-issued mobile devices may connect to the firm's (wired and wireless) network.

Best Practices

- To prevent interference with colleagues, employees should take personal calls outside of the office. Unless it's an emergency, it is best for employees to take personal calls during their break time.
- Company-issued mobile devices should only be used for business purposes.
- Employees should not use their company-issued phone as a personal phone.
- Employees should take care of their computer-issued mobile device as they were their own. The mobile device must be returned un-damaged.

Password Policy

Policy

1. Employees must protect their credentials at all time.
2. Employees should not share their credentials with anyone.
3. Each employee is required to change their password every six (6) months. The new password cannot be the same as one of the last twenty-four (24) passwords. Once the user log into their Windows workstation, they will be prompted to change their password. They will not be able to use their workstation until the password has been changed.
4. Employees must not contact the system administrator to have their password changed to something easier to remember. The purpose of a secure password is to make it more difficult for people to guess the password.
5. Employees must not send the username and password to anyone within the same email. A separate email containing just the password is acceptable.

Best Practices

- When creating a password, it should consist of, at least, eight (8) characters in length, a number, and a combination of upper and lower case letters. Example password: 2Rwe1$eupZ
- Passwords should not be kept in a publicly accessible area such as on the desk or under the computer monitor. All employees are encouraged to either remember their password(s) or store them in a location that cannot be accessed by others.
- Employees should change their password, at least, once every six (6) months.
- Use two-factor authentication when possible.
- Employees should ask the IT department to reset their password if they cannot remember it.

Anti-Virus Policy

All computers running the Windows operating system must have a modern anti-virus software installed. The IT department is responsible for updating and maintaining the anti-virus software on all workstations.

Policy

1. Employees must not disable the anti-virus software that is installed on their workstation.
2. Each computer must stay on, at least, twice a week in order for the anti-virus definition updates, computer scans, and Windows security updates to run effectively at night.
3. Employees must not interrupt any anti-virus scanning or update activity. In most cases, the updates and scanning are done on a nightly basis – no user interaction should be required.
4. Employees must never force quit the anti-virus software in their computer.
5. Employees should notify the IT department if the anti-virus software is affecting the performance for their computer.
6. Employees must notify the IT department of any email or file that the anti-virus software had detected.
7. Employees must not turn off (or pause) ESET Endpoint Security's Presentation Mode. The Presentation Mode feature alerts the user (in real-time) when a virus is detected.

Best Practices

- Employees should never open any email attachments from unknown senders (especially MS Word and Excel documents). If an employee is unsure whether it's safe or not to open an attachment, he/she must contact his/her supervisor first. The supervisor must then contact the system administrator.
- The ESET Endpoint Security software has a plug-in for Microsoft Outlook, which scans actively scans emails for viruses, spam, and phishing messages. EJR employees must not attempt to open any email attachments that has been moved to the "Infected Items" folder (within Outlook).

Windows and Workstation Policy

The workstations within the firm runs on either Windows 7 Pro or Windows 10 Pro. No other operating systems has been approved by the IT department.

To log into the firm's network, users must use the credentials that were given to them by the IT department. If they are logging in for the first time, they will be asked to change the password on Windows.

The account will be automatically locked after five (5) consecutive login failures. The user must contact the IT department to have their password reset if their account has been locked.

Policy

1. Employees must get approval from the IT department before attempting to install any software on their workstation.
2. Employees should lock their workstation (by pressing Windows + "L" keys) before leaving their desk.
3. Employees must not attempt to edit the Windows registry data for any reason.
4. Employees must not attempt to access other users' data in the same workstation.
5. Employees must not connect to open Wi-Fi networks (in the area) using their workstation.
6. Employees must shut down their workstation every Friday night to save energy, allow Windows to apply updates, and help prevent any unwanted intrusions.
7. Employees are required to change their password according to the Password Policy.
8. The IT department must deactivate the user's account once they exit the firm.

Best Practices

- Do not plug in any portable drives into the USB port.
- Never reveal your password to anyone (other than a member of the IT department).
- Do not browse inappropriate websites using your workstation.
- Always allow Windows to apply security updates.

Remote Access Policy

The firm permits remote connections via three methods: Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP) and LogMeIn. Access must be approved by the department manager and provisioned by a member of the IT department.

A VPN allows users to connect to a network via a secure tunnel. Remote users must be connected via this protocol to get access to the shared network directories.

Users may connect to the firm's SFTP server by using a username/password combination or public key. After five (5) unsuccessful login attempts, the IP address will be blocked for 24 hours.

LogMeIn is a software (by LogMeIn, Inc.) that allows users to access their computers remotely from anywhere. The firm has enabled two-factor authentication ("2FA") to prevent unauthorized users from connecting to the network. Using the 2FA method, a one-time code will be sent to the users' cell phone during the login process. Users will not be able to login without entering the special code. If a user cannot login after two attempts, they will need to talk to a LogMeIn agent to reset their password.

Policy

1. LogMeIn privileges are only given to employees who cannot come into the office. They will only have access to their workstation in the office -- nothing more.
2. Employees must not share their remote access credentials with anyone.
3. Employees must not connect remotely using an unsecured connection such as a public Wi- Fi network. I.e. Starbucks
4. LogMeIn users can only connect to the machine(s) that are assigned to their account.
5. SFTP users can only access the directories that are assigned to them.
6. Employees should not download anything to their personal computer when connected remotely.
7. Remote users should not conduct any personal (and/or illegal) business while connected to the organization's network.
8. Employees must log off or close the remote connection window immediately when they're done doing their work.
9. Employees should contact the system administrator if they cannot log into their account remotely.

Wireless Internet (Wi-Fi) Policy

The firm maintain two (2) wireless (Wi-Fi) networks: public and private. Both networks are secured by the WPA2 (Wi-Fi Protected Access 2) with AES (Advanced Encryption Standard) encryption.

The public network is available to all EJR guests and employees. It does not connect to the firm's internal network. A user that is connected to the firm's public network will not be able to access any of the firm's network drives.

To access the firm's private Wi-Fi, employees must get approval from the firm's IT department.

Policy

- Employees must not connect to the firm's Wi-Fi network using their personal mobile device(s).
- Employees must not use the Wi-Fi network to download music, videos, or large applications.
- Employees must not share the Wi-Fi credentials with anyone in the firm without approval from the IT department.

Best Practices

- Be careful when you connect to public (free) Wi-Fi networks -- hackers can easily see what you've what you've submitted in a web form, email, and your browsing history.
- Always connect to a secure Wi-Fi network. A secure Wi-Fi network requires a password with modern encryption (AES).
- Follow the Internet Usage Policy.

Social Media

There are many risks involved with social media. Social media includes, but not limited to Facebook, LinkedIn, Twitter, Instagram, Pinterest, Tumblr, Google Plus, and blogs. It is important that employees know what they can and cannot post on social media. The firm does not allow access to social media websites (other than LinkedIn) from the Haverford office.

The IT department maintains control of the official EJR and EJP Twitter accounts: *eganjonesrating*, *eganjonesproxy* and *theproxyexperts*. All accounts are kept in "active" status, but configured as private, however, to prevent someone else from trying to use the firm's name.

Policy

1. Employees must not use social media to post confidential information such as ratings, client information or any other financial information.
2. Employees must not use a social media website or app during work hours.
3. Employees must not create any social media account on behalf of the firm without prior approval from the firm's management team and compliance department.
4. Employees must not post anything on social media on behalf of the firm without prior approval from the Compliance department.
5. Employees must not include any of their personal social media web addresses in their work email signature.
6. EJR and EJP's marketing teams should not retweet (or repost) each other's message(s) on social media.

Best Practices

- Keep in mind that social media is available to everyone in the world.
- Do not post anything that you think you'll regret later on.

Data Protection & Retention Policy

To comply with local, federal, and/or European laws, the firm must store data securely. Specifically, personal (client) data should not be shared with any third-party firm or posted publicly without the client's consent.

According to the new EU's General Data Protection Regulation (GDPR) rules (effective May 25th, 2018), we must:

- obtain consent from clients before we can store their data or use it for marketing/communication purposes
- delete their data after they submit a request to us
- send them a copy of their data (in CSV or XLS format) after they submit a request to us
- tell them how we are tracking them on our website through our privacy policy

The Data Protection Officer (DPO) is the firm's IT department. The DPO's role is to ensure that any type of data is kept securely.

Policy

1. Keep client data secured.
2. Delete the data if a client sent a deletion request unless the firm need it for legal purposes.
3. Make data available to clients if they request for it.
4. Do not store more than personal data than you need.
5. Make sure that any web service we use are GDPR compliant for European customers.
6. Make sure the data is up-to-date and is accurate as possible.
7. Make sure the privacy policy is updated and posted on the firm's website.
8. Get consent from the client before storing their personal information in a database (such as Outlook, Excel, Act, Salesforce, Quickbooks, and PP Tracker) or using it for marketing purposes.

Cybersecurity Breach Response Procedures

In an event of an information security breach, the firm must do the following:

1. Discover the breach. Find out what exactly was leaked and who it may have affected.
2. Investigate and remediate. Find out who the perpetrator is. Apply any security holes if applicable. Prevent future breaches
3. Assemble internal response team. The response team should consist of people from the compliance, legal, IT, public relations, and operations departments.
4. Contact third-party cybersecurity experts. Third-party experts will have a better eye on things. They should be able to help remediate any other risks involved.
5. Notify all affected clients. If applicable, the firm must notify all affected clients about the breach. The clients must know exactly what they need to do next. If their credentials were compromised, they must be reset immediately by EJR.
6. Respond to inquiries. The compliance and IT department will need to work together to respond to any concerns or complaints clients may have regarding the breach.
7. Create incident report. An incident report must be created for each incident.
8. Resume business. After all of the first eights (8) steps above are complete, business may resume as normal.

Disciplinary Consequences

For an action that constitutes a breach of security, violation of the confidentiality policy or cause of an accident the employee may face severe disciplinary repercussions up to and including termination.

Appendix A – Data Classification

DATA CLASS	RISK LEVEL	DEFINITION	EXAMPLES
Confidential	High	Only accessible to EJR management staff and board members	Sensitive personal identification information Individuals' bank information Clients' financial statements
Restricted	High	Normally accessible only to specified EJR staff members	Employee personal information Drive access information Clients' contractual agreements
Internal	Moderate	Normally accessible only to all or specified EJR staff members	Rating model Proxy Writer Employee policies and procedures
Public	Low	Accessible to all members of the public	Company contact information All EJR public facing websites Newsletters