## Protecting Consulting Project Data

Consulting project data is stored and protected according to a minimum set of criteria, with more stringent protections applied for sensitive data and at the request of the customers. For most consulting engagements, proposals and project information is stored on an internal file server, with access restricted to EBP employees and officers, or on Microsoft Teams channels available to all current EBP employees and officers.

In the event a customer or teaming partner needs access to a file server for collaborations, a unique project Microsoft Teams site is created, located on a secure Microsoft cloud server, with access permissions set by the assigned EBP project lead. Access to this web-based site may include select EBP employees and client representatives and partners, including other consulting organizations.

## Controlling access to data

Internal file server access is controlled by key-controlled access to premises and Windows log-in credentials to access company-owned and -maintained hardware. Password protected VPN access and company-owned and -maintained hardware can also be used to remotely access the EBP's servers.

EBP's Teams sites are accessed through Microsoft Office 365 usernames and passwords managed based on EBP's global password policies. All access requires multi-factor authentication. Based on Office 365 usernames, access to specific Teams sites can be controlled to a limited number of members. This is used to limit access to project data when needed for project data security and confidentiality/privacy reasons. Private channels within project-specific teams can further limit sensitive data access to only essential staff for analysis and management of such data.

## Protecting data confidentiality

All EBP employees sign an employment agreement to hold all client and partner information in strictest confidence and not to disclose data and project information, regardless of sensitive nature, to any person or entity outside the firm. However, for projects that collect and analyze sensitive data, including personally identifiable information (PII), EBP, at a client's request, may have all staff with access to project files or project leadership with responsibility for other staff sign project specific non-disclosure and data use agreements reiterating their commitment to protecting data and using it within the agreed bounds for the project. These confidentiality agreements can also remind staff of the penalties involved in disclosing confidential data.

EBP considers PII to include at a minimum the names of individuals, addresses, birth dates, social security numbers, bank account and payment information, as well as any other information a client requests to be treated as confidential or proprietary information.

For elevated access control, EBP leverages Microsoft Teams to create a project-specific site and control team membership to only those staff associated with the project. When project teams are larger than the number of staff working directly with data, it can be stored in a private channel for increased access control.

## Disposal of consulting project data

EBP maintains standard procedures for the final disposition of all research study records at the completion of each research project. While EBP's standard practice is to archive all final data and analysis projects to allow reproducible analysis in the case of future client inquiries, EBP will at the request of clients and data providers delete confidential or private data either immediately after analysis of the data is complete or at completion of the task or project in which the data is used. Any data containing PII or every identified as confidential or proprietary by a client will not be archived in any file storage system to which access is less controlled than that in place during the project. If there are paper data records, confidential products, or other physical media that would disclose confidential information and risk the privacy of individuals this is destroyed. EBP can issue a "certificate of record of destruction" following file or physical media removal. The certificate would be signed by the project Data Custodian (the project manager if not otherwise named or an officer of the firm).