Betterment at Work

Your 401(k) is secure with us

When employers choose Betterment at Work, their 401(k) plan will be protected by a robust cybersecurity program, which follows the Department of Labor's 12 guidelines for retirement plan providers, also known as Cybersecurity Program Best Practices.

How we keep your employee accounts safe

1

Documented cybersecurity program

We operate a comprehensive security program, built to identify and control operational risks related to confidentiality, integrity, and availability of information assets.

2

Annual risk assessments

Betterment at Work performs annual assessments, using the NIST Cybersecurity Framework.

3

Annual third-party audits

We use several independent third-parties to test and audit key internal controls, including:

SOC AUDIT REPORTS

Betterment at Work engages an independent public accounting firm to perform independent audits each year, testing the operating effectiveness of identified key internal controls over financial reporting. Audit reports are made available to clients, including a SOC 2 Type II with coverage for the security program, as well as a SOC 1 Type II report with coverage for internal controls specifically relevant to us.

PENETRATION TESTING

We engage qualified independent firms to perform network and application layer testing, with a specific focus on the applications we develop that constitute our product. This testing is performed annually and whenever selected changes may introduce new risks.

4

Clearly defined team roles and responsibilities

Our security team includes qualified information security professionals. Detailed roles and responsibilities are defined within our program.

5

Strong company-wide access controls

Betterment at Work employs logical access controls based on the principle of least privilege (which refers to the minimum amount of access privileges necessary to perform a job function). Users are granted access to our information systems based on their role or discretionary access. Additional requirements, such as authentication controls, the use of multi-factor authentication, periodic user reviews and re-certification, and controls protecting remote access, are defined in our policy.

6 Assets or data stored in the cloud or managed by a third-party service provider

We use third party relationships to provide Betterment at Work services. For instance, some of our production infrastructure and storage is provided by Amazon Web Services (AWS). We have a shared security model with AWS, wherein Betterment and Amazon are each responsible for security controls while using the cloud services.
All third-party relationships at Betterment are subject to a robust third party risk management (TPRM) program that requires due diligence and ongoing monitoring.

7 Cybersecurity awareness training

All of our employees are assigned mandatory training for security and privacy awareness upon hire, and annually thereafter. We provide additional training to personnel whose role may allow for elevated levels of risk.

8 Secure System Development Life Cycle program (SDLC)

Betterment designs, builds, and operates software. Controls related to managing risks are in place throughout the software development lifecycle.

For example, a Secure Design Review (Threat Modeling) evaluates the threats and controls related to new software development. Threat modeling is performed based on risk, and includes a review of the product or new feature requirements, user stories, or other scope documentation.

9 Business resiliency program

We have a Business Continuity and Disaster Recovery (BC/DR) program, which establishes the use of a Business Impact Analysis (BIA) to identify recovery targets for key business processes. Following a disaster, we have recovery plans in place. Recovery plans also contemplate key third-party relationships, whose BCP/DR capabilities are assessed during third-party risk management due diligence. These recovery plans are tested annually.

10 Encryption of sensitive data stored and in-transit

Encryption in transit is always in place, using TLS 1.2 or higher. Client connections to 401k.betterment.com are negotiated, and require TLS 1.2 or 1.3.
Non-public information, which is always subject to Betterment data classification controls, is encrypted at rest. Data at rest encryption relies on documented key management practices, and includes both encryption by the cloud provider and selected application and database-level encryption. Workstations used by Betterment employees use whole-disk encryption.

11 Strong technical controls to ensure best security practices

Betterment implements and maintains technical security controls required to manage security risks. These are evaluated during risk assessment processes, and we continue to make investments in order to address emerging risks.

Network Security is managed by segmenting networks within Amazon Web Services. Betterment monitors and controls communications at network boundaries.

We've implemented network segmentation (e.g., firewalls or comparable technology) to restrict connections between networks of different security zones. A web application firewall (WAF) is in place to control external access, at the application layer, to web and mobile endpoints used by Betterment. A Security Incident Event Manager (SIEM) is used to collect security events and analyze them. A third-party managed security services provider (MSSP) is engaged for first-tier monitoring and escalation, and our security engineers have an on-call rotation to investigate potential security incidents.

12 Responsiveness to cybersecurity incidents or breaches

Betterment has established processes for security incident detection and response, which includes:

- Informing law enforcement
- Notifying Betterment's appropriate insurer
- Investigating the incident
- Giving affected clients, including Betterment at Work plans and participants, the information necessary to mitigate harm. This notice considers regulatory and contractual timeliness considerations, as well as mandatory breach notifications where appropriate
- Remediating the problems that caused the incident
- Performing post-incident analysis to learn and identify control enhancements with the aim of reducing the likelihood or impact of future incidents

Interested in learning more about security at Betterment?

Interested in learning more about security at Betterment?
Betterment is happy to provide the following documents through its Trust Portal at trust.betterment.com (please note: access will require a non-disclosure agreement):

- Betterment at Work's SOC 1 audit, which covers our security and operational controls
- Betterment's SOC 2 audit, which covers the Security trust principal

Key policies, including the Information Security Policy, Risk Management Framework, and Business Continuity/Disaster Recovery Policy

Get in touch:

For sales inquiries: (845) 210-4371 or 401k@betterment.com
For existing clients: plansupport@betterment.com

Betterment 450 West 33rd Street, FL 11 New York, NY 10001