

Environment Variables Checklist

Purpose

This checklist helps you configure all required environment variables for the Mindful Champion application in production.

✓ Configuration Checklist

● CRITICAL - Must Have (App won't start without these)

☐ DATABASE_URL

- **Current Status:** ✓ Configured
- **Purpose:** PostgreSQL connection string for all database operations
- **Where to get it:** Your database provider (Supabase, Railway, etc.)
- **Format:** `postgresql://USER:PASSWORD@HOST:PORT/DATABASE?options`
- **Example:** `postgresql://user:pass@db.host.com:5432/mydb?connect_timeout=30`
- **Used by:** Prisma, all database queries
- **Security:** CRITICAL - Never expose publicly

☐ NEXTAUTH_SECRET

- **Current Status:** ✓ Configured
- **Purpose:** Encrypts JWT tokens and session data
- **Where to get it:** Generate with `openssl rand -base64 32`
- **Format:** 32+ character random string
- **Example:** `zRLB8vJYT6iqfo0jb2lZTwbbkLrck6uR`
- **Used by:** NextAuth authentication system
- **Security:** CRITICAL - Rotate every 90 days

☐ NEXTAUTH_URL


- **Current Status:** ✓ Configured
- **Purpose:** Base URL for OAuth callbacks and redirects
- **Where to get it:** Your production domain
- **Format:** `https://yourdomain.com` (no trailing slash)
- **Example:** `https://mindful-champion-2hzb4j.abacusai.app`
- **Used by:** NextAuth, OAuth providers
- **Security:** Must match actual domain

☐ GMAIL_USER


- **Current Status:** ✓ Configured
- **Purpose:** Gmail account for sending all emails
- **Where to get it:** Your Gmail account
- **Format:** `email@gmail.com`
- **Example:** `welcomefrommc@mindfulchampion.com`

- **Used by:** Email notification system, goal reminders
- **Security:** Medium - Can be public but keep password secret
- **Documentation:** See `GMAIL_SETUP.md`


□ **GMAIL_APP_PASSWORD**

- **Current Status:**  Configured
- **Purpose:** SMTP authentication for Gmail
- **Where to get it:** <https://myaccount.google.com/apppasswords>
- **Format:** 16-character string (no spaces)
- **Example:** `mtj1wqxxgxpzuqwe`
- **Used by:** Nodemailer SMTP transport
- **Security:** CRITICAL - Never expose
- **Requirements:** 2-factor authentication must be enabled
- **Documentation:** See `GMAIL_SETUP.md`

□ **CRON_SECRET**

- **Current Status:**  Configured (provided)
- **Purpose:** Authenticates cron job requests
- **Where to get it:** Generate with `openssl rand -base64 32` OR use provided
- **Format:** Base64 encoded string
- **Value:** `jYEyBMds0rDgrmmAPi8yuUisg2C0zDfqnf/8/1VkJCo=`
- **Used by:** Vercel Cron jobs, notification scheduling
- **Security:** CRITICAL - Protects cron endpoints from unauthorized access
- **Documentation:** See section below

□ **ABACUSAI_API_KEY**

- **Current Status:**  Configured
- **Purpose:** Access Abacus.AI for Coach Kai and video analysis
- **Where to get it:** <https://abacus.ai/app/profile/apikey>
- **Format:** 32-character hex string
- **Example:** `19050ea030924f3dbc432d96ecbd0a89`
- **Used by:** Coach Kai AI, video analysis engine
- **Security:** CRITICAL - Never expose

□ **NEXT_PUBLIC_APP_URL**

- **Current Status:** Needs verification
 - **Purpose:** Public app URL for email links and redirects
 - **Where to get it:** Your production domain
 - **Format:** `https://yourdomain.com` (no trailing slash)
 - **Example:** `https://mindfulchampion.com`
 - **Used by:** Email links, QR codes, social sharing
 - **Security:** Public - OK to expose
-

🟡 IMPORTANT - Core Features (Features won't work without these)

☐ AWS_REGION

- **Current Status:** ✅ Configured
- **Purpose:** AWS region for S3 bucket
- **Where to get it:** Your AWS S3 bucket settings
- **Format:** AWS region code
- **Example:** `us-west-2`
- **Used by:** Video upload, file storage
- **Security:** Public - OK to expose

☐ AWS_BUCKET_NAME

- **Current Status:** ✅ Configured
- **Purpose:** S3 bucket for video/file storage
- **Where to get it:** AWS S3 Console
- **Format:** Bucket name
- **Example:** `abacusai-apps-bucket-name`
- **Used by:** Video uploads, user content storage
- **Security:** Public - OK to expose (bucket should have proper IAM)

☐ AWS_FOLDER_PREFIX

- **Current Status:** ✅ Configured
- **Purpose:** Organizes files within S3 bucket
- **Where to get it:** Define your own (e.g., `6482/`)
- **Format:** `folder-name/` (with trailing slash)
- **Example:** `6482/`
- **Used by:** File organization in S3
- **Security:** Public - OK to expose


☐ AWS_PROFILE

- **Current Status:** ✅ Configured
- **Purpose:** AWS credentials profile name
- **Where to get it:** Set in AWS credentials file
- **Format:** Profile name string
- **Example:** `hosted_storage`
- **Used by:** AWS SDK authentication
- **Security:** Medium - Keep private


☐ AWS_CONFIG_FILE

- **Current Status:** ✅ Configured (platform-specific)
- **Purpose:** Path to AWS credentials file
- **Where to get it:** Platform-specific (usually auto-set)
- **Format:** File path
- **Example:** `/opt/hostedapp/configs_credentials/credential`
- **Used by:** AWS SDK authentication
- **Security:** System-level - Platform managed


❑ STRIPE_PUBLISHABLE_KEY

- **Current Status:**  Configured
- **Purpose:** Client-side Stripe integration
- **Where to get it:** <https://dashboard.stripe.com/apikeys>
- **Format:** `pk_test_` or `pk_live_`
- **Example:** `pk_test_51SKk0o3ZJvYimaqq...`
- **Used by:** Frontend payment forms
- **Security:** Public - Safe to expose (read-only)


❑ STRIPE_SECRET_KEY

- **Current Status:**  Configured
- **Purpose:** Server-side Stripe operations
- **Where to get it:** <https://dashboard.stripe.com/apikeys>
- **Format:** `sk_test_` or `sk_live_`
- **Example:** `sk_test_51SKk0o3ZJvYimaqqeGB...`
- **Used by:** Server payment processing
- **Security:** CRITICAL - Never expose


❑ STRIPE_WEBHOOK_SECRET

- **Current Status:**  Needs update (has placeholder)
- **Purpose:** Validates Stripe webhook events
- **Where to get it:** <https://dashboard.stripe.com/webhooks>
- **Format:** `whsec_...`
- **Example:** `whsec_abc123xyz...`
- **Used by:** Payment webhook processing
- **Security:** CRITICAL - Never expose

❑ STRIPE_PREMIUM_PRICE_ID

- **Current Status:**  Configured
- **Purpose:** Stripe price ID for Premium subscription
- **Where to get it:** <https://dashboard.stripe.com/products>
- **Format:** `price_...`
- **Example:** `price_1SKk9Z3ZJvYimaqqDm90FY5e`
- **Used by:** Subscription checkout
- **Security:** Public - OK to expose

❑ STRIPE_PRO_PRICE_ID

- **Current Status:**  Configured
- **Purpose:** Stripe price ID for Pro subscription
- **Where to get it:** <https://dashboard.stripe.com/products>
- **Format:** `price_...`
- **Example:** `price_1SKk9Z3ZJvYimaqqfqeKzkm`
- **Used by:** Subscription checkout
- **Security:** Public - OK to expose

❑ NEXT_PUBLIC_STRIPE_PREMIUM_PRICE_ID

- **Current Status:**  Configured

- **Purpose:** Client-side access to Premium price ID
- **Where to get it:** Same as STRIPE_PREMIUM_PRICE_ID
- **Format:** price_...
- **Used by:** Frontend subscription UI
- **Security:** Public - OK to expose

☐ NEXT_PUBLIC_STRIPE_PRO_PRICE_ID

- **Current Status:** ☒ Configured
- **Purpose:** Client-side access to Pro price ID
- **Where to get it:** Same as STRIPE_PRO_PRICE_ID
- **Format:** price_...
- **Used by:** Frontend subscription UI
- **Security:** Public - OK to expose

NOTIFICATION SYSTEM VARIABLES

☐ NOTIFICATION_EMAIL

- **Current Status:** Needs to be set
- **Purpose:** "From" address for notification emails
- **Format:** email@domain.com
- **Example:** welcomefrommc@mindfulchampion.com
- **Used by:** Goal reminders, video analysis notifications
- **Security:** Public - OK to expose

☐ SUPPORT_EMAIL

- **Current Status:** Needs to be set
- **Purpose:** Support inquiry destination
- **Format:** email@domain.com
- **Example:** support@mindfulchampion.com
- **Used by:** Contact forms, support tickets
- **Security:** Public - OK to expose

☐ PARTNERS_EMAIL

- **Current Status:** Needs to be set
- **Purpose:** Partner communication
- **Format:** email@domain.com
- **Example:** partners@mindfulchampion.com
- **Used by:** Partner outreach, integrations
- **Security:** Public - OK to expose

☐ SPONSORS_EMAIL

- **Current Status:** Needs to be set
- **Purpose:** Sponsor communication
- **Format:** email@domain.com
- **Example:** sponsors@mindfulchampion.com
- **Used by:** Sponsor applications, offers

- **Security:** Public - OK to expose

☐ EMAIL_FROM

- **Current Status:** ☒ Configured
- **Purpose:** Default “from” address for all emails
- **Format:** email@domain.com
- **Example:** welcomefrommc@mindfulchampion.com
- **Used by:** All outgoing emails
- **Security:** Public - OK to expose

☐ EMAIL_REPLY_TO

- **Current Status:** Needs to be set
- **Purpose:** Reply-to address for email responses
- **Format:** email@domain.com
- **Example:** dean@mindfulchampion.com
- **Used by:** All outgoing emails
- **Security:** Public - OK to expose

☐ EMAIL_NOTIFICATIONS_ENABLED

- **Current Status:** Needs to be set
- **Purpose:** Global email notification toggle
- **Format:** true or false
- **Example:** true
- **Used by:** Notification system
- **Security:** Public - OK to expose

OPTIONAL - Nice to Have (Graceful degradation)

☐ GOOGLE_CLIENT_ID

- **Current Status:** Not configured
- **Purpose:** Google OAuth sign-in
- **Where to get it:** <https://console.cloud.google.com/apis/credentials>
- **Format:** Long alphanumeric string
- **Used by:** Google sign-in feature
- **Security:** Public - OK to expose

☐ GOOGLE_CLIENT_SECRET

- **Current Status:** Not configured
- **Purpose:** Google OAuth authentication
- **Where to get it:** <https://console.cloud.google.com/apis/credentials>
- **Format:** Alphanumeric string
- **Used by:** Google sign-in feature
- **Security:** SECRET - Never expose

☐ TWILIO_ACCOUNT_SID

- **Current Status:** ☒ Configured
- **Purpose:** Twilio SMS service

- **Where to get it:** <https://console.twilio.com/>
- **Format:** AC followed by alphanumeric
- **Example:** AC7feddafe6d788cf548dc5d99300b2a66
- **Used by:** SMS notifications (optional feature)
- **Security:** Medium - Keep private

☐ TWILIO_AUTH_TOKEN

- **Current Status:** ☒ Configured
- **Purpose:** Twilio authentication
- **Where to get it:** <https://console.twilio.com/>
- **Format:** Alphanumeric string
- **Used by:** SMS notifications
- **Security:** CRITICAL - Never expose

☐ TWILIO_PHONE_NUMBER

- **Current Status:** ☒ Configured
- **Purpose:** Twilio sending number
- **Where to get it:** Twilio console
- **Format:** +1XXXXXXXXXX
- **Example:** +18556429735
- **Used by:** SMS notifications
- **Security:** Public - OK to expose

☐ RESEND_API_KEY

- **Current Status:** ☒ Configured
- **Purpose:** Alternative email service (backup to Gmail)
- **Where to get it:** <https://resend.com/api-keys>
- **Format:** re_ followed by alphanumeric
- **Example:** re_Syxd3DX8_246jEmL7Lb1aYAXJnm76FziF
- **Used by:** Email service (alternative to Gmail)
- **Security:** SECRET - Never expose

☐ YOUTUBE_API_KEY

- **Current Status:** Not configured
- **Purpose:** YouTube video integration
- **Where to get it:** <https://console.cloud.google.com/apis/credentials>
- **Used by:** Media center, tournament streams
- **Security:** Public - OK to expose (with restrictions)

☐ BETS_API_KEY

- **Current Status:** Not configured
- **Purpose:** Live pickleball scores
- **Where to get it:** <https://betsapi.com/>
- **Used by:** Live scores section
- **Security:** SECRET - Keep private

☐ PICKLEBALL_API_TOKEN

- **Current Status:** Not configured

- **Purpose:** Official pickleball tournament data
 - **Where to get it:** <https://api.pickleball.com/>
 - **Used by:** Tournament information
 - **Security:** SECRET - Keep private
-

Quick Actions

Immediate Actions Needed

1. ☐ Set `NEXT_PUBLIC_APP_URL` to production domain
2. ☐ Set `STRIPE_WEBHOOK_SECRET` to actual webhook secret
3. ☐ Set `NOTIFICATION_EMAIL` for goal reminders
4. ☐ Set `SUPPORT_EMAIL` for support inquiries
5. ☐ Set `PARTNERS_EMAIL` for partner communications
6. ☐ Set `SPONSORS_EMAIL` for sponsor communications
7. ☐ Set `EMAIL_REPLY_TO` to `dean@mindfulchampion.com`
8. ☐ Set `EMAIL_NOTIFICATIONS_ENABLED` to `true`
9. ☐ Verify `CRON_SECRET` is set to provided value

Recommended Actions

1. ☐ Set up Google OAuth (if desired)
 2. ☐ Configure external API keys (YouTube, BetsAPI, etc.)
 3. ☐ Enable analytics and monitoring
 4. ☐ Review and rotate secrets (NEXTAUTH_SECRET, CRON_SECRET)
-

Security Checklist

- ☐ All `.env` files are in `.gitignore`
 - ☐ No secrets committed to version control
 - ☐ Different values for dev/staging/prod
 - ☐ API keys have proper restrictions (domains, IPs)
 - ☐ Database has SSL enabled
 - ☐ S3 bucket has proper IAM policies
 - ☐ Rotate secrets every 90 days
 - ☐ Monitor failed authentication attempts
 - ☐ Set up alert for suspicious activity
-

Additional Documentation

- **Gmail Setup:** See `EMAIL_SETUP.md`
- **Notification System:** See `NOTIFICATION_SYSTEM.md`
- **S3 Configuration:** See AWS S3 setup guide
- **Deployment:** See `DEPLOYMENT_GUIDE.md`







- **Security:** See `SECURITY_BEST_PRACTICES.md`
-

Verification

Run the verification script to check your configuration:

```
npm run verify-env
```

This will:

-  Check all required variables are set
 -  Validate formats
 -  Test database connection
 -  Test email sending
 -  Test S3 access
 -  Report missing/invalid variables
-

Last Updated: December 3, 2025

Status: Ready for Production Configuration